

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.⁷
G06F 12/14

(11) 공개번호 특2001-0076222
(43) 공개일자 2001년08월11일

| | |
|------------|--|
| (21) 출원번호 | 10-2000-0062787 |
| (22) 출원일자 | 2000년10월25일 |
| (30) 우선권주장 | 2000-4271 2000년01월13일 일본(JP) 2000-4272 2000년01월13일 일본(JP) 2000-4273 2000년01월13일 일본(JP) |
| (71) 출원인 | 가시오게산키 가부시키가이샤 가시오 가즈오 |
| (72) 발명자 | 일본국 도쿄도 시부야구 혼마치 1초메 6번 2고 오츠카모토미 |
| (74) 대리인 | 일본국도쿄도다치카와시나시키토1-13-12-603 손은진 |

심사청구 : 있음

(54) 휴대단말장치, 서버장치, 시스템 및 그 프로그램기록매체

요약

본 발명은 휴대단말장치에 의하여 휴대형 데이터기록매체를 액세스할 때의 시큐리티대책을 강구한 시큐리티관리수법의 제안에 관한 것으로서,

본 발명의 과제는 중요정보를 포함한 데이터를 휴대단말(2)로부터 분리 가능한 DB카드(3)에 보관해 두고 단말과 매체의 대응지움에 의해 그 데이터에 대한 액세스 외에 이 카드 자체에 대한 액세스도 불가능하게 하는 다중시큐리티라는 만전의 대책을 강구하는 것으로, 분실, 도난, 악의 등에 의한 카드내의 중요정보의 누설을 확실하게 방지할 수 있도록 하는 것이고, 휴대단말장치(2)가 DB카드(3)를 액세스할 때, 이 카드내의 「하드식별번호」와 자기의 「하드식별번호」를 대조하고, 그 대조결과에 의거하여 해당 DB카드에 대한 액세스가부를 결정하며, 그 결과 해당 카드에 대한 액세스가 허가되었을 때에는 또한 휴대단말장치(2)는 이 카드에 기억되어 있는 「소프트식별번호」와 자기의 「소프트식별번호」를 대조하고, 그 대조결과에 의거하여 해당 카드내의 모바일로의 액세스가부를 결정하는 것을 특징으로 한다.

도면도

도1

도2

서버장치, 휴대단말장치, DB카드, 소프트식별번호

도3

도면의 간단한 설명

도 1은 시큐리티관리시스템의 전체구성을 나타낸 블록도.

도 2는 단말그룹대응의 DB카드(3)를 설명하는 동시에 휴대단말장치와 사용자의 대응관계를 설명하기 위한 도면.

도 3은 다중시큐리티를 개념적으로 나타낸 도면.

도 4는 서버장치측에 설치되어 있는 설정데이터(11)의 구성과 그 설정내용, 마스터DB파일(12), DB대응기본AP(13)를 나타낸 도면.

도 5는 각 DB카드(3)에 기입된 내용을 나타낸 도면.

도 6은 각 휴대단말장치(2)의 내장메모리에 기입된 내용을 나타낸 도면.

도 7은 서버장치(1), 휴대단말장치(2)의 전체구성을 나타낸 블록도.

도 8A는 서버장치(1)가 설정데이터(11)에 대하여 설정을 실시하는 경우의 동작을 나타낸 흐름도.

도 8B는 도 8A에 이어지는 설정동작을 나타낸 흐름도.

도 9A는 서버장치(1)가 마스터DB나 커스터마이징AP 등을 DB카드(3)에 기입하여 배포하는 경우의 동작을 나타낸 흐름도.

BEST AVAILABLE COPY

- 도 9B는 도 9A에 이어지는 배포동작을 나타낸 흐름도.
 도 10A는 마스터DB를 나타낸 도면.
 도 10B는 마스터DB로부터 「레코드추출조건」에 의하여 추출된 레코드를 나타낸 도면.
 도 10C는 각 추출레코드로부터 「추출대상필드」에 의하여 변경된 변경 후의 레코드구성을 나타낸 도면.
 도 11은 휴대단말장치(2)측에 있어서 전원투입에 따라 실행개시되는 흐름도.
 도 12는 스텝C7(검색뷰어 기동)시의 동작을 상세히 서술하기 위한 흐름도.
 도 13A는 스텝D16(DB대응의 커스터마이즈AP 기동)시의 동작을 상세히 서술하기 위한 흐름도.
 도 13B는 도 13A에 이어지는 커스터마이즈AP 기동시의 동작을 상세히 서술하기 위한 흐름도.
 도 14는 서버장치(1)에 있어서, 일상업무의 수행에 따라서 변경된 DB카드내의 모빌DB를 수집하여 서버내의 마스터DB를 갱신하는 경우의 회수동작을 나타낸 흐름도이다.

※도면의 주요부분에 대한 부호의 설명

- | | |
|--------------|-------------------|
| 1: 서버장치 | 2: 휴대단말장치 |
| 3: DB카드 | 4: 카드리더/라이터 |
| 5: 시리얼케이블 | 11: 설정테이블 |
| 12: 마스터DB파일 | 13: 마스터DB대응의 기본AP |
| 21, 21A: CPU | 22: 기억장치 |
| 23: 기록매체 | 24: RAM |
| 25: 전송제어부 | 26: 입력부 |
| 27: 표시부 | |

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 휴대단말장치에 의하여 휴대형 데이터기억매체를 액세스할 때의 시큐리티대책을 강구한 시큐리티관리수법의 제안에 관한 것이다.

근래 콤팩트디스크나 메모리카드 등의 휴대형 기억매체는 대용량화, 소형화가 진행되어 대량의 데이터베이스를 휴대형 기억매체에 격납함으로써 각종 데이터베이스를 자유롭게 운반할 수 있게 되어 오고 있다.

여기에서 영업담당자가 휴대단말장치를 지참하고 일상의 영업활동을 행하는 경우에 있어서, 휴대단말장치는 그 내장메모리의 용량이 적기 때문에 각종 업무처리용의 데이터베이스의 일부 또는 전부를 휴대형 기억매체에 격납하도록 하고 있다. 여기에서 영업담당자는 단말본체에 휴대형 기억매체를 장착하고, 외출처에서 그 기억내용을 액세스하여 표시출력시키거나 데이터갱신 등을 실시하도록 하고 있다.

이 경우 휴대단말장치에 의하여 휴대형 데이터기억매체를 액세스할 때의 시큐리티대책으로서, 입력된 패스워드에 의하여 정당한 단말이용자인지를 인증하도록 하고 있다.

그런데 본래 개인전용기로서의 휴대단말장치에 있어서도 정직원 외에 파견직원, 파트, 아르바이트족도 사용하는 케이스가 증가해 오고 있다. 또 휴대단말장치는 외출처에 운반하여 사용한다는 관계상, 휴대형 기억매체나 휴대단말장치 자체를 외출처에서 분실하거나 도난될 위험성이 있었다. 따라서 휴대형 기억매체나 단말의 내장메모리내에 기밀성이 높은 중요한 기업정보나 개인정보가 격납되어 있는 경우에 분실, 도난, 악의에 의하여 그 중요정보가 타인에게 누설될 염려는 매우 높았다.

즉 종래에 있어서는 휴대단말장치를 주로 외출처에서 사용한다는 관계상, 입력조작을 복잡화한 엄밀한 시큐리티관리보다도 조작의 간소화, 신속성 등의 조작환경을 중시하고 있기 때문에 휴대형 기억매체나 휴대단말장치의 분실이나 도난에 대한 시큐리티대책이나 파견직원, 파트 등에 의한 악의에 대한 시큐리티대책은 충분하지 않고, 사용자패스워드를 알고 있으면, 또는 패스워드의 우발적인 히트에 의하여 누구라도, 어떤 퍼스널컴퓨터로부터도 용이하게 휴대단말이나 기억매체내의 데이터를 액세스할 수 있어서 중요정보가 타인에게 누설되어 버릴 위험성은 매우 높았다.

또 사용자설정제에 의하여 임의로 시큐리티대책을 강구하기 위한 장치를 휴대단말장치 자체에 갖게 해 두는 것은, 반대로 제 3자에 의하여 그 설정부분의 변경도 용이하게 실시할 수 있는 위험성을 포함하게 되어, 그 장치 자체가 안전성을 손상시키는 요인으로 되어 버린다.

발명이 이루고자 하는 기술적 과제

본 발명의 과제는 분실, 도난, 악의 등에 의한 데이터기억매체내의 중요정보의 누설을 확실하게 방지할 수 있는 동시에 시큐리티관리를 위해 사용자에게 특별한 조작을 요구하지 않고, 조작성을 손상하지 않는 확실한 시큐리티관리를 실현할 수 있도록 하는 것이며, 또 정당한 단말, 오퍼레이터 이외의 제 3자에 의한 부정한 액세스를 확실하게 방지할 수 있고, 외출처에서 사용한다는 특질을 고려한, 확실한 시큐리티관

리를 실현할 수 있도록 하는 것이다.

본 발명의 수단은 휴대형 데이터기억매체의 이용을 제한하는 액세스제한정보로서의 제 1 식별정보 및 제 2 식별정보가 기억되어 있는 휴대단말장치에 있어서, 임의의 휴대형 데이터기억매체를 액세스할 때에, 이 데이터기억매체내에 기억되어 있는 제 1 식별정보와 자기의 제 1 식별정보를 대조하고, 그 대조결과에 의거하여 해당 데이터기억매체에 대한 액세스가부를 결정하며, 그 결과 해당 데이터기억매체에 대한 액세스가 허가된 경우에, 이 데이터기억매체내에 기억되어 있는 제 2 식별정보와 자기의 제 2 식별정보를 대조하고, 그 대조결과에 의거하여 해당 데이터기억매체내의 데이터로의 액세스가부를 결정함으로써 상기 제 1 식별정보 및 제 2 식별정보에 의하여 해당 단말장치와의 대응지움에 설정되어 있는 정당한 데이터기억매체인지 아닌지를 다중으로 체크하도록 한 것이다.

본 발명에 따르면, 중요정보를 포함한 데이터를 휴대단말로부터 분리 가능한 휴대형 데이터기억매체에 보관해 두고, 단말과 매체의 대응지움에 의해 그 데이터에 대한 액세스 외에, 이 데이터기억매체 자체에 대한 액세스도 불가능하게 하는 다중시큐리티라는 만전의 대책을 강구하는 것으로, 분실, 도난, 악의 등에 의한 데이터기억매체내의 중요정보의 누설을 확실하게 방지할 수 있는 동시에 시큐리티관리를 위해 사용자에게 특별한 조작을 요구하지 않고, 조작성을 손상하지 않는 시큐리티관리를 실현할 수 있다.

또 중요정보를 포함한 데이터가 기억되어 있는 휴대형 데이터기억매체를 분실하거나 도난된 경우 등에 있어서도, 그 데이터기억매체대응의 정당한 단말인지를 다중으로 체크하거나 정당한 오퍼레이터인지를 체크한다는 만전의 세큐리티대책을 강구하는 것으로 정당한 단말, 오퍼레이터 이외의 제 3자에 의한 부정한 액세스를 확실하게 방지할 수 있으며, 외출처에서 사용한다는 특질을 고려한, 확실한 시큐리티관리를 실현할 수 있다.

또 휴대형 데이터기억매체로의 데이터파일의 기입 외에 데이터기억매체와 그것을 액세스 가능한 휴대단말 장치의 대응지움과, 데이터기억매체와 그것을 이용 가능한 사용자의 대응지움을 서버장치가 일괄하여 실시할 수 있는 동시에, 데이터기억매체에 대한 시큐리티관리를 확실한 것으로 하기 위해 그 대책을 강구하기 위한 장치를 휴대단말장치에 갖게 하지 않으며, 또 시큐리티관리를 위해 사용자에게 특별한 조작을 요구하지 않고, 조작성을 손상하지 않는 확실한 시큐리티관리를 실현할 수 있다.

또 서버장치가 휴대형 데이터기억매체에 데이터파일을 기입할 때에 그 데이터에 효과적인 중복암호화를 실시해 두는 것으로 데이터기억매체를 분실하거나 도난된 경우 등에 있어서, 만일 정당한 단말 이외에 의하여 그 데이터파일로의 액세스까지 다다른 최악의 케이스에도 그 데이터파일의 전모가 해독될 가능성을 없앨 수 있어서 중요정보의 누설을 확실하게 방지할 수 있다.

또 휴대형 데이터기억매체내의 데이터파일을 각 레코드마다 암호화해 두는 것으로 해당 기억매체를 액세스하는 경우에도 암호화된 채의 상태로 실시할 수 있으며, 기억매체의 분실, 도난, 또는 악의 등에 있어서, 만일 정당한 단말 이외가 데이터파일의 액세스까지 다다른 최악의 케이스에도 복호화된 레코드만의 시큐리티가 문제가 될 뿐으로, 그 파일의 전모가 해독될 위험성은 없어서 중요정보의 누설을 확실하게 방지할 수 있다.

또 휴대형 데이터기억매체에 대한 시큐리티관리를 확실한 것으로 하기 위해 데이터기억매체로의 데이터파일의 기입 외에 데이터기억매체와 그것을 액세스 가능한 휴대단말장치의 대응지움을 서버장치가 일괄하여 실시할 수 있는 동시에, 토대가 되는 마스터데이터베이스를 그대로 기입하는 것은 아니고, 마스터데이터베이스로부터 잘라낸 레코드군만으로 이루어지는 모바일데이터파일을 작성하여 기입하는 것으로, 해당 매체대응의 정당한 단말에 대해서도 필요 이상의 정보를 제공하지 않는다는 대책을 강구할 수 있으며, 또 분실, 도난, 악의 등에 의한 데이터기억매체내의 중요정보의 누설을 확실하게 방지할 수 있다.

발명의 구성 및 작용

이하 도 1~도 14를 참조하여 본 발명의 한 실시형태를 설명한다.

도 1은 이 실시형태에 있어서의 시큐리티관리시스템의 전체구성을 나타낸 블록도이다.

이 시큐리티관리시스템은 예를 들면 회사조직에 있어서 회사측에 설치시키고 있는 서버장치(1)와, 각 영업담당자가 지참하는 모바일형의 클라이언트단말(휴대단말장치)(2)과, 이 휴대단말장치(2)에 세트되어 이용되는 휴대형 기억매체(3)를 갖고 있다.

그리고 서버장치(1)측에서 기억관리되고 있는 어플리케이션소프트/데이터베이스 등을 운반 자유로운 휴대형 기억매체(3)를 통해서 휴대단말장치(2)측에 외부제공하도록 하고 있으며, 이 기억매체(3)에 데이터베이스 등을 기입하여 단말장치에 배포할 때에 서버장치(1)는 해당 단말과 기억매체를 대응지우기 위한 정보를 설정하거나 각종 시큐리티대책을 강구함으로써 기억매체(3)내의 어플리케이션소프트/데이터베이스 등이 제 3자에 의하여 부정복사되거나 정보가 누설되는 것을 확실하게 방지하도록 한 것이다.

그리고 각 영업담당자는 외출처에서 휴대형 기억매체(3)내의 어플리케이션소프트/데이터베이스를 액세스하면서 영업활동을 실시하고, 그리고 하루의 영업종료시에 단말본체로부터 휴대형 기억매체(3)를 빼내며, 그것을 서버장치(1)측의 카드리더/라이터(4)에 세트하면 서버장치(1)는 카드리더/라이터(4)를 통하여 기억매체(3)내의 영업기록을 수집처리하도록 하고 있다.

그리고 서버장치(1)와 복수대의 휴대단말장치(2)는 시리얼케이블(5)을 통하여 착탈 자유롭고 접속 가능하게 되어 있다.

휴대형 기억매체(3)는 각종 업무처리용의 어플리케이션소프트나 데이터베이스 등을 기억하는 것으로, 예를 들면 콤팩트플래쉬카드에 의하여 구성되어 있다. 이하 휴대형 기억매체(3)를 모바일데이터베이스카드(DB카드)라 부른다.

여기에서 도면 중 각 DB카드(3)에 붙인 「#A」, 「#B」, 「#C」, ...는 단말명칭 「A」, 「B」, 「C」, ...로 나타내어지는 휴대단말장치(2)에 대응지워진 단말대응의 카드인 것을 나타내고 있다. 또한 이 실시

형태에 있어서는 단말대응의 카드 외에 휴대하는 단말그룹대응의 카드도 존재하는데, 도 1의 예에서는 단말대응의 카드만을 나타내고 있다. 카드리더/라이터(4)는 DB카드(3)를 복수장 동시에 세트 가능한 것으로, 복수의 카드삽입구를 갖고 있다.

그리고 서버 장치(1)는 DB카드(3)를 통하여 휴대단말장치(2)측에 어플리케이션소프트/데이터베이스파일(AP소프트/DB파일)을 배포한다. 즉 서버장치(1)는 DB카드(3)에 기입하는 기입대상, 즉 배포대상의 AP소프트/DB파일을 호출하여 카드리더/라이터(4)에 주고, 그것에 세트되어 있는 1 또는 2 이상의 DB카드(3)에 AP소프트/DB파일을 기입한다.

도 2는 예를 들면 업무그룹 「영업1과」, 「영업2과」, 「프로젝트A」, 「프로젝트B」, ...에 대응하는 단말그룹과, 이 단말그룹대응의 DB카드(3)의 관계를 나타내는 동시에 단말과 사용자의 대응관계를 나타낸 것이다.

즉 도면 중 「#A1」, 「#A2」, 「#A3」로 나타내는 각 DB카드(3)는 단말명칭이 「A1」, 「A2」, 「A3」인 각 휴대단말장치(2)가 속하는 단말그룹대응의 기억매체이고, 마찬가지로 「#B1」, 「#B2」, ...로 나타내는 DB카드(3)는 단말명칭이 「B1」, 「B2」, ...인 각 휴대단말장치(2)가 속하는 단말그룹대응의 기억매체이며, 동일그룹내의 각 DB카드(3)는 그 그룹에 속하는 각 휴대단말장치(2)에서 공통하여 사용할 수 있도록 되어 있다.

또 어떤 휴대단말을 이용할 수 있는 권한을 갖는 사용자는 한사람으로 한정되지 않고 복수의 사용자가 1대의 휴대단말장치를 공유하여 사용할 수 있으며, 또 어떤 사용자는 복수대의 휴대단말장치를 이용할 수 있는 권한을 갖고 있다. 예를 들면 단말그룹A에 있어서, 단말명칭 「A1」으로 나타내어지는 휴대단말장치와 사용자 「UA1」 ~ 「UA4」의 대응관계가 정의되고, 또 단말명칭 「A2」로 나타내어지는 휴대단말장치와 사용자 「UA1」 ~ 「UA3」의 대응관계가 정의되어 있으며, 이들 사이에 한하여 이용관계가 있는 것을 나타내고 있다. 이 경우 복수사용자에 의한 공유사용이 가능한 단말대응의 각 DB카드에는 공유사용이 가능한 각 사용자에 대응하여 그 인증정보(패스워드)가 설정된다.

도 3은 이 실시형태의 특징인 다중시큐리티관리의 장치를 개념적으로 나타낸 도면이다. 이 다중시큐리티관리는 휴대단말장치(2)가 임의의 DB카드를 액세스할 때, 또는 DB카드(3)가 임의의 단말장치에 의하여 액세스될 때의 시큐리티처리를 나타낸 것으로, 이 다중시큐리티를 대별하면 4가지의 시큐리티층으로 이루어진다.

즉 이 다중시큐리티관리의 장치는 제 1 시큐리티층(DB카드시큐리티)과, 제 2 시큐리티층(패스워드인증)과, 제 3 시큐리티층(소프트시큐리티)과, 제 4 시큐리티층(데이터베이스다중암호화)으로 이루어져 있다.

제 1 시큐리티층(DB카드시큐리티)은 휴대단말장치(2)가 임의의 DB카드를 액세스할 때에, 또는 DB카드(3)가 임의의 단말장치에 의하여 액세스될 때에 있어서, 단말 및 카드내에 각각 기억되어 있는 제 1 식별정보(후술하는 하드식별번호)끼리를 대조하고, 그 대조결과에 의거하여 해당 카드 자체에 대한 액세스가부를 결정하는 체크처리이다. 이 체크처리는 단말의 전원투입시에 있어서, 카드내에 격납되어 있는 기본소프트의 기능에 의하여 실행게시된다.

여기에서 「하드식별번호」는 휴대단말장치(2)와 DB카드(3)를 대응지워 두기 위해 미리 휴대단말장치(2)나 DB카드(3)에 기입된 것이다. 즉 서버장치(1)가 휴대단말장치(2)나 DB카드(3)에 기입하기 위한 내용을 미리 테이블설정해 둘 때에 「하드식별번호」는 동일그룹에 속하는 휴대단말장치(2) 중 어느 쪽인가 1대의 단말로부터 판독한 고유의 단말식별정보(제조번호)에 따라서 생성된 것으로, 서버장치(1)는 그룹대응의 각 휴대단말장치(2) 및 그들 단말에서 이용되는 각 DB카드(3)내에 하드식별번호를 각각 기입한다. 따라서 동일그룹에 속하는 각 휴대단말장치(2) 및 각 DB카드(3)내에는 각각 동일한 하드식별번호가 공통의 액세스제한정보로서 각각 기입된다.

제 2 시큐리티층(패스워드인증)은 상기한 DB카드시큐리티체크의 결과, 해당 카드 자체에 대한 액세스가 허가된 경우에 입력된 사용자인증정보(패스워드)에 의거하여 정당한 오퍼레이터인지를 대조하는 체크처리이다.

이 경우의 대조에는 암호화패스워드가 이용된다. 즉 이 암호화패스워드는 입력된 패스워드를 소정의 방법으로 암호화한 것으로, 단말대응의 각 DB카드(3)내에 사용자 고유의 인증정보로서 각각 기입된다. 이 경우 그 단말에 대하여 액세스권한이 부여되어 있는 복수의 사용자가 존재하고 있는 경우에는 각 사용자마다 암호화패스워드의 기입이 실시된다.

또한 이 제 2 시큐리티층에 있어서는 DB카드(3)의 이용시에 있어서, 사용자패스워드가 입력되었을 때에 잘못된 패스워드가 연속하여 몇 회나 반복해서 오입력된 경우, 그 반복입력회수가 미리 설정되어 있는 한도값(후술하는 뷰어비작동설정회수)에 도달한 것이 판별되면, 그 이후 검색뷰어(패스워드입력을 재촉하는 표시 등의 초기화면 표시)를 비작동으로 함으로써 패스워드입력을 받아들이지 않는 상태로 하는 시큐리티처리도 아울러서 실시하도록 하고 있다.

제 3 시큐리티층(소프트시큐리티)은 휴대단말장치(2)가 임의의 DB카드를 액세스할 때에, 또는 DB카드(3)가 임의의 단말장치에 의하여 액세스될 때에 있어서, 단말 및 카드내에 각각 기억되어 있는 제 2 식별정보(후술하는 소프트식별번호)끼리를 대조하고, 그 대조결과에 의거하여 해당 카드내의 데이터베이스(모빌DB)에 대한 액세스가부를 결정하는 체크처리이다.

이 「소프트식별번호」는 DB카드(3)내의 데이터베이스와 그것을 이용 가능한 휴대단말장치(2)를 대응지워 두기 위해 미리 휴대단말장치(2)나 DB카드(3)에 기입된 것이다. 즉 서버장치(1)가 휴대단말장치(2)나 DB카드(3)에 기입하기 위한 내용을 미리 테이블설정해 둘 때에 「소프트식별번호」는 동일그룹에 속하는 휴대단말장치(2) 중 그 어느 쪽인가 1대의 단말로부터 판독한 고유의 단말식별정보(제조번호)와, 그 그룹명칭, 소정의 마스터명칭에 따라서 생성된 것으로, 서버장치(1)는 그룹대응의 각 휴대단말장치(2) 및 그들 단말에 대응지워져 있는 각 DB카드(3)내에 소프트식별번호를 각각 기입한다.

제 4 시큐리티층(데이터베이스다중암호화)은 DB카드를 분실하거나 도난된 경우에, 만일 제 3자가 그 DB카드에 대하여 액세스할 수 있었다고 해도 DB카드내의 데이터베이스를 다중암호화에 의하여 그 해독을 방지하는 시큐리티대책을 나타내고 있다.

여기에서 서버장치(1)는 DB카드(3)에 데이터베이스를 기입하여 배포할 때에 배포처의 그룹에 대응지워져 있는 마스터데이터베이스를 그대로 카드에 기입하는 것은 아니고, 마스터데이터베이스로부터 해당 그룹의 업무내용에 따라서 필요한 데이터내용만을 잘라내고, 잘라낸 데이터로 이루어지는 그룹대응의 데이터베이스(모빌DB)를 작성하도록 하고 있는데, 그 때 작성된 모빌DB의 파일관리정보, 즉 각 파일의 격납위치를 나타내는 FAT(File Allocation Table)를 스크램블처리(암호화처리)하도록 하고 있다.

이 FAT스크램블처리는 스크램블처리용으로서 임의로 생성된 암호키(스크램블키)를 이용하여 실시되는데, 스크램블처리를 어떠한 수법으로 실시하는지는 임의이다.

또 서버장치(1)는 DB카드(3)내에 모빌DB를 기입할 때에 임의로 생성한 레코드암호화키를 이용하여 1레코드, 필드마다 모빌DB의 각 레코드를 개별로 암호화하도록 하고 있다. 이와 같이 모빌DB는 다중암호화되어 DB카드내에 기입된다.

도 4는 서버장치(1)측에 설치되어 있는 설정테이블(11), 마스터DB파일(12), 마스터DB대응의 기본AP(13)를 나타내고 있다. 이 설정테이블(11)은 서버장치(1)가 DB카드(3)나 휴대단말장치(2)에 기입하기 위한 각종 내용을 미리 설정해 두는 것으로, 이 실시형태에 있어서는, DB카드(3)로의 기입을 휴대단말장치(2) 자체에 실시하게 하는 것은 아니고, 서버장치(1)가 일괄하여 실시하도록 하고 있다.

설정테이블(11)은 그룹 「영업1과」, 「영업2과」, 「프로젝트A」, 「프로젝트B」, ...와 같은 단말그룹마다 각종 설정에러리어를 갖는 구성으로 되어 있다. 이 각 그룹마다의 설정에러리어에 세트된 내용은 해당 그룹대응의 각 휴대단말장치(2)나 각 DB카드(3)내에 기입된다. 또한 도 4에서는 단말그룹으로서 「영업1과」, 「영업2과」, 「영업3과」를 예시한 경우를 나타내고 있다.

우선 각 그룹대응의 설정에러리어에는 「그룹명칭」 외에 상기한 「하드식별번호」, 동일그룹에 속하는 단말의 합계 「설정인수」, 그 각 단말마다의 「단말명(1)」, 「단말명(2)」, ... 동일그룹내에 있어서, 그 단말을 사용할 수 있는 권한을 갖는 사용자의 합계 「사용인원수」가 각각 설정되어 있다.

또한 그룹마다 설정되어 있는 「뷰어비작동설정횟수(N)」는 패스워드의 오입력이 연속하여 몇 회나 반복된 경우, 그 이후 검색뷰어를 비작동으로 하기 위해 그룹마다 임의로 설정된 설정횟수이다.

또 사용의 권한을 갖는 각 사용자에 대응지워서 그 「사용자명(1)」, 「패스워드」, 「사용자명(2)」, ...가 설정되어 있다. 또 그룹마다 상기한 「스크램블키(SK)」, 「레코드암호화키(RK)」가 각각 설정되어 있다.

또 기입대상으로서의 각 데이터베이스에 대응지워서 그 「모빌DB명(1)」, 「마스터DB명」, 「레코드추출조건」, 「추출대상필드」, 「모빌DB명(2)」, ...가 설정되어 있다.

「마스터DB명」은 서버장치측에서 기억관리되고 있는 복수의 마스터DB파일(12) 중 해당 그룹의 업무내용 등에 따라서 필요로 하는 마스터DB를 지정하는 것이며, 또 「레코드추출조건」, 「추출대상필드」는 그 마스터DB를 해당 그룹의 업무내용 등에 따라서 수정변경함으로써 그룹대응의 모빌DB를 작성할 때에 사용되는 모빌DB작성용의 조건을 정의하는 것이다.

즉 「레코드추출조건」은 이 마스터DB로부터 소망하는 레코드군을 추출하기 위한 추출조건을 나타내고, 「추출대상필드」는 이 추출레코드군으로부터 소망하는 필드만으로 이루어지는 레코드구성으로 변경하기 위한 필드추출조건을 나타내고 있다. 그리고 「레코드추출조건」, 「추출대상필드」를 마스터DB마다 설정해 둘으로써 해당 그룹의 업무내용이나 휴대단말마다의 처리내용을 만족시키는 고유의 모빌DB가 작성된다.

또 「모빌DB명(1)」, 「모빌DB명(2)」, ...에 대응지워서 「커스터마이즈AP(1)」, 「커스터마이즈AP(2)」, ...가 설정되어 있다. 이 「커스터마이즈AP」는 상기한 모빌DB를 처리하기 위한 어플리케이션 소프트웨어, 마스터DB대응의 기본AP(13)를 모빌DB에 따라서 그 표시형태를 수정변경한 것이다.

이 「대응커스터마이즈AP」에는 상기한 「소프트식별번호」, 「갱신날짜」, 「대응모빌DB명」이 대응설정되어 있다. 이 경우 「소프트식별번호」는 동일그룹내의 각 「커스터마이즈AP」에 공통하여 설정되는데, 「갱신날짜」는 그 기본AP를 수정변경했을 때의 날짜에 따라서 상이하다.

또한 「커스터마이즈AP」의 설정에러리어에 그 AP명만을 세트하도록 해도 좋다. 이 경우에는 해당 커스터마이즈AP 자체는 별도파일에 격납해 두고, 설정테이블(11)내의 대응커스터마이즈AP명에 따라서 해당 어플리케이션소프트 자체를 호출하도록 해도 좋다.

한편 설정테이블(11)에는 각 그룹에 공통하여 각 DB카드에 기입되는 공통의 기입대상으로서 「기본소프트」가 그룹대응설정에러리어와는 별도의 에러리어에 설정되어 있다. 여기에서 「기본소프트」에는 「검색뷰어」, 「FAT스크램블/해제알고리즘」, 「암호화/복호화알고리즘」, 「동작제어관리파일」을 포함하는 구성으로 되어 있다.

「기본소프트」는 휴대단말 장치의 기본적인 동작을 실행제어하기 위한 기본소프트이며, 「검색뷰어」는 기본소프트의 동작에 따라서 초기화면(로그인입력화면)을 표시시키는 소프트웨어이다.

「동작제어관리파일」은 DB대응커스터마이즈AP를 동작제어하기 위한 기본적인 관리정보가 격납되어 있는 파일이다. 이 「동작제어관리파일」은 통상 카드내에 기입되어 있는데, 이 실시형태에 있어서는 패스워드의 오입력이 연속하여 몇 회나 반복된 경우, 그 이후 검색뷰어를 비작동으로 하기 위해 「동작제어관리파일」을 삭제하도록 하고 있으며, 검색뷰어가동시에 이 「동작제어관리파일」이 DB카드내에 존재하고 있는 것을 조건으로 하여 휴대단말장치는 로그인입력화면을 표시시키도록 하고 있다.

도 5는 서버장치에 의하여 각 DB카드(3)에 기입된 내용을 나타내고 있다. 즉 DB카드에는 「하드식별번호

「FAT(스크램블완료)」, 「기본소프트」, 「검색뷰어」, 「FAT스크램블/해제알고리즘」, 「암호화/복호화알고리즘」, 「동작제어관리파일」, 「부여비작동설정횟수」가 기입되어 있다. 「FAT(스크램블완료)」는 해당 DB카드내의 각 모빌DB를 관리하는 관리정보이며, 스크램블처리된 내용인 채 기입되어 있다.

또한 해당 DB카드를 사용 가능한 각 사용자에게 대응하여 「사용자명(1)」, 「암호화패스워드+시간변수키」, 「사용자명(2)」, ...가 기입되어 있는 동시에 「레코드암호화키(RK)」가 기입되어 있다.

또 「모빌명(1)」, 그 실제데이터인 「DB(암호완료)」, 「모빌명(2)」, ...가 기입되고, 또한 모빌DB에 대응지워서 「커스터마이징AP(1)」와, 「소프트식별번호」, 「갱신 날짜」, 「대용모빌명」, 「커스터마이징AP(2)」, ...가 기입되어 있다.

도 6은 각 휴대단말장치(2)의 내장메모리에 기입된 내용을 나타내고 있다. 이 내장메모리에는 도시와 같이 플래쉬ROM, RAM(일시기억메모리)이 설치되어 있다. 이 ROM, RAM은 시큐리티대책도 고려하여 필요최소한의 메모리용량으로 한 구성으로 되어 있다. 즉 이 실시형태에 있어서는, 상기와 같이 어플리케이션, 데이터베이스, 기본소프트 등의 격납장소를 휴대단말장치(2)와 DB카드(3)로 분산하지 않고 DB카드(3)에 어플리케이션, 데이터베이스 외에 기본소프트도 기입하도록 하고 있으며, 휴대단말 자체의 분실, 도난 등에 의한 위험을 해소할 수 있도록 하고 있다.

여기에서 서버장치(1)의 기입동작에 의하여 단말내의 플래쉬ROM에는 상기한 「하드식별번호」, 「소프트식별번호」, 「스크램블키(SK)」가 고정적으로 기억된다. 또 일시기억메모리인 RAM은 「키/데이터입력메러러」, 「FAT판독메러러」, 「레코드메러러」, 「그 밖의 워크메러러」를 갖는 구성으로 되어 있다.

또한 「레코드메러러」는 단말내에 데이터를 남기지 않도록 하기 위해 필요최소한의 데이터, 즉 현재 처리중인 커런트분으로써 레코드분의 데이터를 일시기억하는 구성으로 되어 있다. 또한 도시하지 않지만, 각 휴대단말장치(2)의 내부메모리에는 각각 제조된 단말 고유의 제조번호도 고정적으로 기억되어 있다.

도 7은 서버장치(1), 휴대단말장치(2)의 전체구성을 나타낸 블록도이다. 여기에서 서버장치(1), 휴대단말장치(2)의 구성요소로서 기본적으로 똑같은 것은 동일번호를 붙여서 그 설명을 겸용하는데, 서버장치(1), 휴대단말장치(2)와의 구성요소를 식별하기 위해 서버장치(1)의 구성요소에는 도면 중 「A」를 붙이고, 이하 휴대단말장치(2)의 구성만을 설명하며, 서버장치(1)의 설명은 생략하는 것으로 한다.

CPU(21)는 기억장치(22)내의 오퍼레이팅시스템이나 각종 어플리케이션소프트에 따라서 이 휴대단말장치(2)의 전체동작을 제어하는 중앙연산처리장치이다. 기억장치(22)는 오퍼레이팅시스템이나 각종 어플리케이션소프트 외에 데이터베이스, 문자폰트 등이 격납되고, 자기적, 광학적, 반도체메모리 등에 의하여 구성되어 있는 기록매체(23)나 그 구동계를 갖고 있다. 이 기록매체(23)는 하드디스크 등의 고정적인 매체, 또는 착탈 자유롭게 장착 가능한 CD-ROM, 플로피디스크, RAM카드, 자기카드 등의 휴대형의 매체이다.

또 이 기록매체(23)내의 프로그램이나 데이터는 필요에 따라서 CPU(21)의 제어에 의해 RAM(예를 들면 스태티크RAM)(24)에 로드되거나 RAM(24)내의 데이터가 기록매체(23)에 세이브된다. 또한 기록매체는 서버 등의 외부기기에 설치되어 있는 것이어도 좋고, CPU(21)는 전송매체를 통하여 이 기록매체내의 프로그램/데이터를 직접 액세스하여 사용할 수도 있다.

또 CPU(21)는 기록매체(23)내에 격납되는 그 일부 또는 전부를 다른 기기측으로부터 전송매체를 통하여 입력하고, 기록매체(23)에 신규등록 또는 추가등록할 수도 있다. 즉 컴퓨터통신시스템을 구성하는 다른 기기로부터 통신회선이나 케이블 등의 유선전송로, 또는 전파, 마이크로웨이브, 적외선 등의 무선전송로를 통하여 송신되어 온 프로그램/데이터를 전송제어부(25)에 의하여 수신해서 기록매체(23)내에 인스톨할 수 있다.

또한 프로그램/데이터는 서버 등의 외부기기측에서 기억관리되고 있는 것이어도 좋고, CPU(21)는 전송매체를 통하여 외부기기측의 프로그램/데이터를 직접 액세스해서 사용할 수도 있다.

한편, CPU(21)에는 그 입출력주변디바이스인 전송제어부(25), 입력부(26), 표시부(27)가 버스라인을 통하여 접속되어 있으며, 입출력프로그램에 따라서 CPU(21)는 그들의 동작을 제어한다. 입력부(26)는 키보드나 터치패널, 또는 마우스나 터치입력펜 등의 포인팅디바이스를 구성하는 조작부이며, 문자열데이터나 각종 코멘드를 입력한다.

다음으로 이 한 실시형태에 있어서의 시큐리티관리시스템의 동작을 흐름도를 참조하여 설명한다. 여기에서 이들 흐름도에 기술되어 있는 각 기능을 실현하기 위한 프로그램은 판독 가능한 프로그램코드의 형태로 기록매체(23(23A))에 격납되어 있으며, CPU(21(21A))는 이 프로그램코드에 따라서 동작을 차례로 실행한다. 또 CPU(21(21A))는 전송매체를 통하여 전송되어 온 상기의 프로그램코드에 따른 동작을 차례로 실행할 수도 있다. 즉 기록매체 외에 전송매체를 통하여 외부공급된 프로그램/데이터를 이용해서 이 실시형태 특유의 동작을 실행할 수도 있다.

도 8A 및 도 8B는 서버장치(1)가 설정테이블(11)에 대하여 각종 설정을 실시하는 경우의 동작을 나타낸 흐름도이다.

우선 기본적인 그룹정보를 설정등록하는 처리가 실시된다(스텝A1~A10). 여기에서 오퍼레이터는 입력 가능한 상태에 있어서, 이번 회에 설정하는 그룹분의 「그룹명칭」을 입력지정하는 동시에(스텝A1), 그 그룹내의 단말 「설정횟수」, 사용자 「사용인원수」의 입력을 실시한다(스텝A2). 그리고 지정횟수분의 휴대단말장치(2)와 그 단말에 대응지우는 DB카드(3)를 서버장치(1)에 세트한 후(스텝A3), 세트한 횟수분의 「단말명」을 각각 입력한다(스텝A4).

그러면 서버장치(1)는 세트되어 있는 동일그룹내의 각 단말 중 어느 쪽인가 1대의 단말을 선택지정하고, 그 「제조번호」를 판독하는 동시에(스텝A5), 이 「제조번호」에 의거하여 「하드식별번호」를 생성하고(스텝A6), 설정횟수분의 각 휴대단말장치(2) 및 DB카드(3)에 「하드식별번호」를 각각 기입한다(스텝A7).

또한, 테이블설정시에 있어서, 휴대단말장치/DB카드로의 기입은 「하드식별번호」의 생성시와 후술하는 「소프트식별번호」 생성시 및 「스크램블키(SK)」의 생성시의 경우에 한하여 실시하도록 하고 있다.

다음의 스텝A8에서는 상기와 같이 입력된 「그룹명칭」, 「설정횟수」, 「단말명」, 「사용인원수」 외에 생성한 「하드식별번호」를 설정테이블(11)에 각각 등록하는 처리가 실시된다.

그리고 패스워드불일치에서의 부여비작동횟수로서 임의의 값을 오퍼레이터가 입력하면(스텝A9), 입력된 「부여비작동횟수」는 설정테이블(11)에 등록된다(스텝A10).

이와 같이 하여 그룹기본정보의 설정등록이 끝나면 그 그룹의 사용인원수분의 패스워드를 설정등록하는 처리로 옮긴다(스텝A11~A15).

우선 오퍼레이터는 사용자명을 입력하는 동시에(스텝A11), 그 사용자대응의 패스워드를 입력하면(스텝A12), 입력된 사용자명, 패스워드는 설정테이블(11)에 각각 등록된다(스텝A13). 이에 따라서 일인분의 사용자등록이 끝나면 사용인원수분의 사용자등록이 종료되었는지를 조사하고(스텝A14), 전체 사용자분의 설정이 종료되기까지 상기의 동작을 반복한다.

그리고 사용자등록이 종료되면 다음으로 「스크램블키(SK)」, 「레코드암호화키(RK)」를 설정등록하는 처리로 옮긴다(스텝A15~A17).

우선 「스크램블키(SK)」를 생성하는 동시에(스텝A15), 「레코드암호화키(RK)」를 생성한다(스텝A16). 이 「스크램블키(SK)」는 상기와 같이 모빌DB의 FAT를 스크램블처리할 때에 사용되는 암호키이며, 또 「레코드암호화키(RK)」는 데이터베이스를 1레코드, 필드마다 암호화할 때에 사용되는 암호화키이다. 이 경우의 키생성방법은 임의이며, 그 때마다 무작위로 생성하도록 해도 좋다.

그리고 생성한 「스크램블키(SK)」, 「레코드암호화키(RK)」를 설정테이블(11)에 각각 등록하는 동시에(스텝A17), 생성한 「스크램블키(SK)」를 설정횟수분, 각 휴대단말장치(2)에 각각 기입한다(스텝A18).

다음으로 데이터베이스 및 그에 대응하는 어플리케이션소프트를 설정등록하는 처리로 옮긴다(스텝A20~A34).

우선, 오퍼레이터는 DB카드에 기입하기 위한 「모빌DB명」 및 그 작성의 토대로 되는 「마스터DB명」을 지정입력하면(스텝A20, A21), 이 「모빌DB명」과 함께 「마스터DB명」은 설정테이블(11)에 대응하여 등록된다(스텝A22). 그리고 지정된 마스터DB에 있어서의 파일의 레코드구성이 안내표시된다(스텝A23). 즉 마스터DB의 각 레코드가 도 10A에 나타내는 바와 같이 8필드 「A」, 「B」~「H」의 각 항목으로 구성되어 있는 것으로 하면, 이 레코드분의 각 항목명이 그 나열순으로 안내표시된다.

여기에서 오퍼레이터는 레코드구성의 안내표시를 확인하고 「레코드추출조건」을 지정입력한다(스텝A24). 즉 안내표시되어 있는 레코드구성의 각 필드 중 소망하는 필드를 조건설정대상필드로서 지정한 후, 그 지정필드에 대한 「레코드추출조건」을 지정입력한다. 예를 들면 갱신날자의 항목을 조건설정대상필드로서 지정한 후 1999년 12월 24일 이후에 갱신된 레코드를 「레코드추출조건」으로서 지정한다.

다음으로 레코드구성의 대상으로 하는 필드를 선택지정한다(스텝A25). 예를 들면 안내표시되고 있는 레코드구성의 각 필드 중 소망하는 필드를 「추출대상필드」로서 선택지정한다. 그러면 지정입력된 「레코드추출조건」 및 레코드구성의 「대상필드명」이 해당 모빌DB명에 대응하여 설정테이블(11)에 각각 등록된다(스텝A26).

그리고 해당 그룹에서 사용하는 기입대상으로서의 전체의 모빌DB를 모두 지정했는지를 조사하고(스텝A27), 전체의 지정이 끝나기까지 상기의 동작을 반복함으로써 모빌DB의 설정등록을 실시한다(스텝A20~A27).

이에 따라서 모빌DB의 설정등록이 끝나면 상기와 같이 하여 판독한 「제조번호」와, 해당 그룹내에서 최초로 지정된 「모빌DB명」과, 입력된 「그룹명」에 의거하여 「소프트식별번호」를 생성하는 동시에(스텝A28), 이 「소프트식별번호」를 설정횟수분의 휴대단말장치(2)에 각각 기입한다(스텝A29).

다음으로 이번 회에 설정등록한 각 모빌DB명에 대응지워서 그 커스터마이징AP를 설정등록하는 처리로 옮긴다. 즉 설정등록한 각 모빌DB명 중 그 어느 쪽인가를 오퍼레이터가 지정하면(스텝A30), 지정된 모빌DB명에 대응하는 「마스터DB명」이 판독되고, 이 마스터DB대응의 기본AP(13)를 액세스하여, 해당 모빌DB를 이용하기 위한 표시형태로 이 기본AP를 수정변경함으로써 소망하는 커스터마이징AP를 임의로 작성한다(스텝A31).

예를 들면 해당 모빌DB의 레코드구성에 따라서 어떤 필드를 어떤 위치에 표시시키는지를 지정하거나 각 필드의 표시사이즈 등을 임의로 지정하면서 기본AP를 수정변경함으로써 소망하는 커스터마이징AP를 작성한다.

그리고 작성한 커스터마이징AP에 「소프트식별번호」, 현재의 시스템날자인 「갱신 날짜」, 「대용모빌DB명」을 기입한 후(스텝A32), 이 커스터마이징AP를 설정테이블(11)에 등록한다(스텝A33). 그리고 전체의 커스터마이징AP를 모두 작성등록하기까지(스텝A34) 상기의 동작을 반복한다(스텝A30~A34).

다음으로 전체의 그룹에 대한 설정등록이 종료되었는지를 조사하고(스텝A35), 전체 그룹종료가 판별되기까지 스텝A1으로 되돌아가서 1그룹마다 상기의 동작을 반복한다. 이에 따라서 설정테이블(11)에는 각 그룹에 대응하여 도 4에 나타낸 각종 내용이 설정등록된다. 그 때 1그룹분의 설정등록이 종료될 때마다 다음의 설정등록대상그룹을 지정하고, 그 그룹대응의 휴대단말장치(2), DB카드(3)를 서버장치(1)에 세트한다. 이와 같은 테이블설정시에 의하여 휴대단말장치(2)에는 「하드식별번호」, 「소프트식별번호」, 「스크램블키(SK)」가 각각 기입되고, 또한 DB카드(3)에는 「하드식별번호」, 「소프트식별번호」가 각각 기입된다.

도 9A 및 도 9B는 서버장치(1)가 모빌DB나 대용커스터마이징AP 등을 DB카드(3)에 기입하여 배포하는 경우의 동작을 나타낸 흐름도이다.

우선, 오퍼레이터는 서버 장치(1)에 배포대상인 1 또는 2 이상의 DB카드(3)를 세트한다(스텝B1). 그러면 세트되어 있는 DB카드 중에서 1개의 카드를 선택하고, 그 카드내로부터 「하드식별번호」를 판독하는 동시에(스텝B2), 이 하드식별번호에 의거하여 설정데이터(11)를 검색하고, 해당하는 그룹을 특정해 둔다(스텝B3).

그리고 각 그룹에 공통하여 각 DB카드에 기입되는 공통의 기입대상으로서의 「기본소프트」를 설정데이터(11)로부터 판독하고, 그 DB카드에 기입한다(스텝B4). 이 경우 「기본소프트」에는 「검색뷰어」, 「FAT 스크램블/해제알고리즘」, 「암호화/복호화알고리즘」, 「동작제어관리파일」이 포함되어 있기 때문에 그 들을 포함하여 기입된다.

다음으로 특정한 그룹대응의 「뷰어비작동설정횟수(N)」를 설정데이터(11)로부터 판독하여 DB카드에 기입 한다(스텝B5).

또한 현재의 시스템일시를 취득하고, 이것을 시간변수키로서 특정해 둔다(스텝B6). 그리고 특정그룹의 각 사용자 중 그 선두의 사용자로부터 대응하는 「패스워드」를 판독하고(스텝B7), 상기의 시간변수를 키 로 하여 이 「패스워드」를 암호화한다(스텝B8). 이에 따라서 생성된 암호화패스워드에 「시간변수키」를 부가하여 대응하는 사용자와 함께 DB카드에 기입한다(스텝B9).

그리고 특정그룹의 각 사용자를 모두 다 지정했는지를 조사하고(스텝B10), 모두 다 지정하기까지 스텝B7 으로 되돌아가서 상기의 동작을 각 사용자에게 반복한다. 이에 따라서 전체사용자분의 처리가 종료되면 설정데이터(11)로부터 특정그룹의 「레코드암호화키(RK)」를 판독하여 DB카드에 기입한다(스텝B11).

다음으로 모빌DB를 작성하여 DB카드에 기입하는 처리로 옮긴다.

우선 설정데이터(11)에 등록되어 있는 특정그룹대응의 각 모빌DB명 중 그 선두의 모빌DB명에 대응지워져 있는 마스터DB명에 해당하는 마스터DB파일을 판독해 둔다(스텝B12). 그리고 이 마스터DB명대응의 「레코 드추출조건」, 「추출대상필드」를 각각 취득하고, 이 「레코드추출조건」에 의거하여 마스터DB파일(12)를 검색함으로써 해당 레코드를 추출한다(스텝B13). 즉 도 10B는 이 경우의 구체예를 나타내고, 마스터 DB(도 10A 참조)로부터 「레코드추출조건」에 해당하는 각 레코드군을 잘라냄으로써 해당 그룹의 업무내 용이나 단말의 처리내용에 필요한 레코드군만이 추출된다.

이에 따라서 추출한 각 레코드군을 「추출대상필드」에 의거하여 그 레코드구성을 변경 한다(스텝B14). 도 10C는 이 경우의 구체예를 나타내고, 추출된 레코드군은 그것을 구성하는 각 필드 중 「추출대상필드」에 해당하는 필드만이 잘라내어지고, 잘라내어진 필드만으로 이루어지는 레코드구성으로 변경된다.

다음으로 도 9B의 스텝B15로 옮기고, 상기와 같이 레코드구성을 변경한 후의 각 레코드 필드를 「레코드 암호화키(RK)」에 의거하여 암호화한다. 이 경우 각 레코드 필드를 암호화할 때마다 「레코드암호화키 (RK)」의 값을 갱신함으로써 각각 다른 키를 이용하여 개별로 암호화하도록 하고 있다. 그리고 암호화된 레코드군을 모빌DB파일로서 작성하여 DB카드에 기입한다(스텝B16).

이와 같이 하여 1파일분의 모빌DB를 작성하면 특정 그룹에 대응하여 다른 모빌DB명이 설정등록되어 있는지 를 조사하고(스텝B17), 있으면 스텝B12로 되돌아가서 상기의 동작을 반복한다.

이에 따라서, 특정그룹대응의 각 모빌DB마다 모빌DB파일이 작성되어 DB카드내에 기입되는 동시에, 그 파 일의 적납위치를 나타내는 FAT가 작성되어 DB카드내에 기입된다.

다음으로 모빌DB대응의 커스터마이징AP를 DB카드에 기입하는 처리로 옮긴다. 우선 마스터DB명에 의거하 여 그에 대응지워져 있는 커스터마이징AP를 설정데이터(11)로부터 판독하고(스텝B18), 그에 대응하는 커 스터마이징AP가 DB카드내에 존재하고 있는지를 조사하는데(스텝B19), 최초는 존재하고 있지 않기 때문에 스텝B24로 진행하여 설정데이터(11)내의 현재의 커스터마이징AP를 판독해서 DB카드에 기록한다. 이에 따 라서 DB카드내에는 모빌DB에 대응하여 최신의 커스터마이징AP(「소프트식별번호」, 「갱신 날짜」를 포함 한다)가 신규로 기입된다.

또 DB카드내에 커스터마이징AP가 존재하고 있는 경우이며도(스텝B19), 그 DB카드내의 「갱신날짜」와 현 행의 커스터마이징AP의 「갱신날짜」를 비교하여 양자의 불일치가 판별된 경우(스텝B20), 즉 현재의 커스 터마이징AP가 갱신되어 있는 경우에도 스텝B24로 진행하여 현재의 커스터마이징AP를 DB카드에 기록함으로 써 최신의 커스터마이징AP로 갱신된다. 또한 「갱신날짜」가 일치하는 경우에는 DB카드내의 커스터마이 징AP는 최신의 것이기 때문에 그 갱신은 실시되지 않는다.

그리고 동일그룹내에 다른 커스터마이징AP가 설정되어 있는지를 조사하고(스텝B21), 있으면 스텝B18으로 되돌아가서 다음의 커스터마이징AP를 판독하고, 이하 똑같은 처리를 반복한다.

그리고 커스터마이징AP의 기입이 끝나면 DB카드내의 모빌DB의 각 파일적납위치를 나타내는 FAT를 「스크 램블키(SK)」를 이용하여 스크램블화한다(스텝B22).

이에 따라서 DB카드 1장분의 기입처리가 끝나면 미기입의 DB카드가 달리 있는지를 판별하고(스텝B23), 다 른 DB카드가 세트되어 있으면 도 9A의 스텝B2로 되돌아가고, 미기입의 DB카드 중에서 그 1개를 지정하여 상기의 동작을 반복한다. 이에 따라서 서버 장치에 세트되어 있는 각 DB카드에는 도 6에 나타난 내용이 각각 기입된다.

이와 같이 하여 기본소프트, 사용자정보, 모빌DB, 대응커스터마이징AP 등이 기입된 DB카드는 그룹마다 해 당 사용자에게 배포된다.

도 11은 휴대단말장치측에 있어서 전원투입에 따라 실행게시되는 흐름도이다.

우선 휴대단말장치에 DB카드가 세트되어 있는 상태에 있어서, 전원이 ON되면 DB카드내의 기본소프트에 의 거하여 기본동작이 개시된다(스텝C1). 그러면 상기한 제 1 시큐리티층의 DB카드시큐리티처리가 실행된다. 즉 DB카드로부터 「하드식별번호」를 판독하고(스텝C2), 해당 단말내의 「하드식별번호」와

대조한다(스텝C3).

이 결과 양자가 일치하는 경우에는(스텝C4), 해당 단말과 카드는 정당한 대응관계에 있기 때문에 DB카드 내의 스크램블완료(FA)를 단말측에 판독하고, 이것을 도 6에서 나타낸 RAM내의 「FA판독에머리어」에 세트하며(스텝C5), 이 「FA」를 단말내의 「스크램블키(SK)」를 이용하여 그 스크램블을 해제한다(스텝C6), 그리고 검색뷰어를 기동시킨다(스텝C7).

또 해당 단말과 카드가 정당한 대응관계에 없는 경우에는 「하드식별번호」의 불일치가 판별되기 때문에 하드에러표시를 실시한 후(스텝C8) 전원을 강제로 OFF하여(스텝C9) 에러종료로 된다.

도 12는 도 11의 스텝C7(검색뷰어 기동)시의 동작을 상세히 서술하기 위한 흐름도이다.

우선 상기한 제 2 시큐리티층의 패스워드인증처리에 있어서, 그 전단계로서의 시큐리티처리가 실행된다. 즉 휴대단말 장치는 검색뷰어 기동시에 DB카드를 액세스하여 카드내에 「동작제어관리파일」이 존재하고 있는지를 체크한다(스텝D1). 여기에서 상기한 바와 같이 패스워드의 오입력이 연속하여 몇 회나 반복된 경우, 그 이후 검색뷰어를 비작동으로 하기 위해 「동작제어관리파일」을 삭제하도록 하고 있다. 따라서 「동작제어관리파일」의 존재유무를 체크하고, 그것이 존재하고 있지 않으면 비작동메시지를 표시시킨 후(스텝D10) 전원을 강제로 OFF하여(스텝D11) 에러종료로 된다.

한편 「동작제어관리파일」이 존재하고 있으면 그것을 조건으로 하여 로그인입력화면을 표시시켜서 사용자명, 패스워드입력을 재촉하는 메시지를 표시한다(스텝D2). 여기에서 오퍼레이터가 자기의 「사용자명」, 「패스워드」를 입력하면(스텝D3), DB카드내의 「사용자명」 대응의 암호화패스워드를 판독하고(스텝D4), 이 암호화패스워드를 「시간변수」를 키로 하여 복호화한다(스텝D5), 그리고 입력된 패스워드와 복호화된 패스워드를 대조한다(스텝D6).

그 결과 양자의 불일치가 판별된 경우에는(스텝D7) 그 불일치횟수를 경신하는 동시에, 그 경신값과 미리 그룹마다 설정되어 있는 「뷰어비작동설정횟수(N)」를 비교하고, 패스워드의 오입력이 연속하여 N회 반복되었는지를 체크하며(스텝D8), N회 미만이면 로그인입력화면으로 되돌아가서(스텝D2) 그 재입력을 받아들인다.

지금 패스워드의 오입력이 연속하여 N회 반복된 것이 판별된 경우에는(스텝D8) 「동작제어관리파일」을 삭제하는 동시에(스텝D9), 비작동메시지를 표시시킨 후(스텝D10) 전원을 강제로 OFF하여(스텝D11) 에러종료로 된다.

또 패스워드의 오입력이 연속하여 N회 반복되기 전에 있어서, 패스워드가 일치하고, 정당한 오퍼레이터인 것이 판별된 경우에는(스텝D7), 우선 상기한 제 3 시큐리티층의 소프트웨어시큐리티처리가 실시된다. 즉 DB 카드내에 기입되어 있는 각 커스터마이징AP의 메뉴화면이 일람표시되기 때문에 이 메뉴화면 중에서 오퍼레이터가 소망하는 커스터마이징AP를 선택지정하면(스텝D12), 선택된 커스터마이징AP에 포함되어 있는 「소프트식별번호」를 DB카드내로부터 판독하고(스텝D13), 자기의 단말내의 「소프트식별번호」와 대조한다(스텝D14). 그 결과 양자의 불일치가 판별된 경우에는(스텝D15) 비작동메시지표시를 실시하는 동시에(스텝D16), 전원을 강제로 OFF하여(스텝D11) 에러종료로 된다.

한편 「소프트식별번호」를 대조한 결과 양자의 일치가 판별된 경우에는 선택된 커스터마이징AP를 개시하고, 그에 따른 어플리케이션처리를 실행개시시킨다(스텝D16).

도 13A 및 도 13B는 도 12의 스텝D16(커스터마이징AP 기동)시의 동작을 상세히 서술하기 위한 흐름도이다.

우선 처리메뉴표시가 실시된다(스텝E1). 이 경우의 메뉴화면에는 「키검색」, 「추가」, 「종료」의 각 메뉴항목이 표시되고, 그 중에서 소망하는 메뉴항목을 선택지정하면(스텝E2), 선택항목을 조사하고(스텝E3, E13), 그에 따른 처리로 옮긴다.

여기에서 메뉴항목 「키검색」이 선택된 경우에 있어서, 검색키(예를 들면 상품명이나 거래처명 등)가 입력되면(스텝E4) DB카드로부터 「레코드암호화키」를 판독하고, 이 검색키를 「레코드암호화키(RK)」로 암호화한다(스텝E5), 그리고 DB카드내의 모빌DB를 암호화된 검색키를 이용하여 검색하고(스텝E6), 그 키에 해당하는 레코드를 추출하는데, 일치하는 키가 없으면(스텝E7) 메뉴표시화면으로 되돌아가서(스텝E1) 검색키의 재입력이 가능하게 된다.

지금 키검색의 결과 일치하는 키가 있으면(스텝E7) 스텝E8으로 옮기고, 해당 모빌DB로부터 검색키에 해당하는 레코드를 판독하여, 도 6에서 나타낸 RAM내의 「레코드에머리어」에 기입한다. 그리고 이 레코드를 「레코드암호화키(RK)」로 복호화하며(스텝E9), 그 레코드내용을 표시출력시키는 동시에(스텝E10), 처리메뉴표시가 실시된다(스텝E11).

이 경우의 메뉴화면에는 「정정」, 「삭제」, 「종료」의 각 메뉴항목이 표시되기 때문에 그 중에서 소망하는 메뉴항목을 선택지정한다(스텝E12). 그러면 선택항목을 조사하여(도 16의 스텝E20, E26) 그에 따른 처리로 옮긴다.

즉 메뉴항목 「정정」이 선택된 경우에 있어서(스텝E20), 정정데이터가 입력되면, 그에 따라서 레코드내용을 정정하는 처리가 실시된다(스텝E21). 그리고 레코드정정이 실시된 것을 나타내기 위해 그 정정레코드에 「정정플래그」를 세트하는 동시에(스텝E22), 정정레코드를 「레코드암호화키(RK)」를 이용하여 암호화하고(스텝E23), 이 암호화레코드를 해당 모빌DB내의 원래의 레코드에 기록한다(스텝E24).

이에 따라서 레코드정정이 종료되면, 그 단말내로부터 해당 레코드를 삭제해 둔다(스텝E25). 즉 도 6에서 나타낸 RAM내의 「레코드에머리어」를 클리어한다.

또 메뉴항목 「삭제」가 선택된 경우에는(스텝E26) 해당 레코드의 데이터부를 삭제하고, 그 레코드에 「삭제플래그」를 세트하며, 해당 모빌DB내의 원래의 레코드에 기록한다(스텝E27). 그리고 단말내로부터 해당 레코드를 삭제해 둔다(스텝E25).

한편 도 13A의 스텝터에서의 처리메뉴화면에 있어서, 「추가」가 선택된 경우에는 스텝터14로 옮겨서 신규 레코드의 입력작성처리가 실시된다. 그리고 레코드추가인 것을 나타내기 위해 신규레코드에 「추가플래그」를 세트하는 동시에(스텝터15), 신규레코드를 「레코드암호화키(RK)」를 이용하여 암호화하고(스텝터16), 이 암호화레코드를 해당 모바일DB내에 추가한다(스텝터17).

이에 따라서 레코드추가가 종료되면 그 단말내로부터 해당 레코드를 삭제한다(스텝터25).

또한 스텝터에서의 처리메뉴화면에 있어서, 「종료」가 선택된 경우에는 단말내의 「FAT」를 삭제한다(스텝터18), 즉 도 6에서 나타낸 RAM내의 「FAT판독메모리」의 내용을 클리어한다. 그리고 그 단말내의 레코드를 삭제한다(삭제E25).

이와 같이 하여 휴대단말 장치측에서는 DB카드에 격납되어 있는 모바일DB의 파일내용이 일상업무의 수행에 따라서 갱신된다.

도 14는 서버 장치에 있어서, 일상업무의 수행에 따라서 변경된 DB카드내의 모바일DB를 수집하여 서버내의 마스터DB를 갱신하는 경우의 동작(회수동작)을 나타낸 흐름도이다.

우선 오퍼레이터가 회수대상인 DB카드를 서버 장치에 세트하면(스텝터F1), 이 DB카드로부터 「하드식별번호」를 판독하고(스텝터F2), 이 「하드식별번호」에 의거하여 설정테이블(11)을 참조해서 그에 해당하는 그룹을 특정한다(스텝터F3). 그리고 DB카드로부터 「스크램블키(SK)」를 판독하고, DB카드내의 FAT를 「스크램블키(SK)」를 이용하여 스크램블해제한다(스텝터F4).

또 DB카드로부터 모바일DB를 판독하고(스텝터F5), 이 DB파일의 각 레코드 필드를 「레코드암호화키(RK)」를 이용하여 복호화한다(스텝터F6). 이 경우에 있어서도 각 레코드 필드를 복호화할 때마다 「레코드암호화키(RK)」의 값을 갱신함으로써 각각 다른 키를 이용하여 복호화를 실시하도록 하고 있다.

그리고 복호화한 DB파일내에 변경 레코드가 존재하는지를 「정정플래그」, 「삭제플래그」, 「추가플래그」의 유무에 의거하여 조사하고(스텝터F7), 변경레코드가 있으면, 즉 어느 쪽인가의 「플래그」가 부가되어 있는 레코드가 존재하고 있으면, 그 모바일DB에 대응하는 서버장치내의 마스터DB를 특정하고(스텝터F8), 해당 모바일DB로부터 판독한 변경레코드에서 그에 부가되어 있는 「플래그」의 종류에 따라서 마스터DB내의 해당 레코드를 갱신하는 처리를 실시한다(스텝터F9, F10).

즉 해당하는 레코드내용을 정정하는 정정처리, 해당 레코드의 데이터부를 삭제하는 삭제처리, 신규레코드를 추가하는 추가처리를 실시한다. 이와 같은 마스터DB의 레코드갱신 처리는 모바일DB내의 전체의 변경레코드에 대하여 실시된다(스텝터F9~F11). 그리고 다른 모바일DB가 DB카드내에 있으면(스텝터F12), 그 모바일DB에 대하여 상기의 동작을 반복한다(스텝터F5~F12).

도 15의 흐름

이상과 같이 이 한 실시형태에 있어서는, 휴대단말장치가 DB카드를 액세스할 때 이 카드내의 「하드식별번호」와 자기의 「하드식별번호」를 대조하고, 그 대조결과에 의거하여 해당 DB카드에 대한 액세스가부를 결정하고, 그 결과 해당 카드에 대한 액세스가 허가되었을 때에 이 카드에 기억되어 있는 「소프트식별번호」와 자기의 「소프트식별번호」를 대조하고, 그 대조결과에 의거하여 해당 카드내의 모바일DB로의 액세스가부를 결정하도록 했기 때문에 단말과 매체의 대응지움에 의해 그 모바일DB에 대한 액세스 외에, 이 카드 자체에 대한 액세스도 불가능하게 하는 다중시큐리티라는 만전의 대책을 강구할 수 있다.

이에 따라서 분실, 도난, 악의 등에 의하여 DB카드내의 모바일DB가 타인에게 누설되는 것을 확실하게 방지할 수 있다. 또 시큐리티관리를 위해 특별한 조작을 요구하지 않고, 조작성을 손상하지 않는 시큐리티관리를 실현할 수 있다. 즉 DB카드를 휴대단말장치에 장착하는 것만으로 자동적으로 시큐리티관리가 실행되기 때문에 DB카드이용시에 사용자는 시큐리티대책을 전혀 인식하지 않아도 좋으며, 쓰기 편리함을 손상하지 않고 확실한 시큐리티관리를 실현할 수 있다.

이 경우 중요정보를 포함한 모바일DB를 휴대단말로부터 분리 가능한 DB카드만에 보관해 두도록 했기 때문에 휴대단말만을 분실하거나 도난되었다고 해도 시큐리티상 전혀 문제는 없고, 또 DB카드를 분실하거나 도난된 경우에도 그 카드로의 액세스는 정당한 단말밖에 할 수 없도록 한 장치를 갖고 있기 때문에 모바일DB에 대한 액세스는 물론 DB카드 자체에 대한 액세스도 불가능하게 되며, 그 시큐리티는 매우 높은 것으로 된다.

또 휴대단말장치는 임의의 DB카드를 액세스할 때 이 카드내의 「하드식별번호」와 자기의 「하드식별번호」를 대조하고, 그 대조결과에 의거하여 해당 카드에 대해서 그 액세스가 허가되어 있는 정당한 단말인지를 체크하고, 정당한 단말인 경우에는 사용자패스워드의 입력을 받아들임 가능하게 하고, 입력된 패스워드와 해당 카드내의 패스워드를 대조하여, 그 대조결과에 의거하여 정당한 사용자인지를 체크하고, 정당한 사용자인 경우에 그 DB카드내의 「소프트식별번호」와 자기의 「소프트식별번호」를 대조하고, 그 대조결과에 의거하여 해당 카드내의 모바일DB에 대하여 그 액세스가 허가되어 있는 정당한 단말인지를 체크하도록 했기 때문에 카드를 분실하거나 도난된 경우 등에 있어서, 그 카드내용의 정당한 단말인지를 다중체크하거나 정당한 오퍼레이터인지를 체크한다는 만전의 시큐리티대책을 강구할 수 있다.

즉 만일 「하드식별번호」에 의한 제 1 시큐리티층이 뚫어져도 제 2 시큐리티층의 패스워드대조에 의하여 보호할 수 있으며, 또한 제 2 시큐리티층이 뚫어져도 제 3 시큐리티층의 「소프트식별번호」에 의하여 보호할 수 있기 때문에 정당한 단말, 오퍼레이터 이외의 제 3자에 의한 부정액세스를 확실하게 방지할 수 있는 동시에, 외출처에서 사용한다는 특질을 고려한, 확실한 시큐리티관리를 실현할 수 있다.

이 경우 패스워드의 오입력이 연속하여 몇 회나 반복된 경우 「동작제어관리파일」을 삭제하도록 하고 있기 때문에, 그 이후 검색부여는 비작동으로 되어 「하드식별번호」에 의한 제 1 시큐리티층과 똑같이 카드 자체에 대한 액세스가 물리적으로 불가능하게 되어 제 3 시큐리티층으로의 침입을 확실하게 방지할 수 있다.

또 서버 장치(1)는 DB카드로의 모빌DB 등을 기입할 때에 DB카드와 그것을 액세스 가능한 휴대단말 장치의 대응지움과, DB카드와 그것을 이용 가능한 사용자의 대응지움을 일괄하여 실시하도록 하기 때문에 그 설정작업을 효율 있게 실시할 수 있는 동시에, DB카드에 대한 시큐리티관리를 확실한 것으로 하기 때문에, 그 대책을 강구하기 위한 장치를 휴대단말장치 자체에 갖게 하지 않고, 또 시큐리티관리를 위해 사용자에게 특별한 조작을 요구하지 않고, 조작성을 손상하지 않는 확실한 시큐리티관리를 실현할 수 있다.

한편 휴대단말장치에 의하여 이용되어야 할 모빌DB를 대응의 DB카드에 대하여 기입하는 서버 장치는 기입 대상인 DB파일내의 각 레코드를 암호화하고, 이 암호화된 DB파일의 FAT를 해제 가능한 형태로 스크램블처리하며, 스크램블처리된 모빌DB를 DB카드에 기입하도록 하기 때문에 모빌DB에 효과적인 중복암호화를 실시할 수 있다. 따라서 만일 정당한 단말 이외에 의하여 그 모빌DB로의 액세스까지 다다른 최악의 케이스에도, 그 모빌DB를 복호화하지 않으면 모빌DB의 일부조차도 해독될 가능성, 하물며 그 전모가 해독될 가능성은 없어서 중요정보의 누설을 확실하게 방지할 수 있다.

또한 「하드식별번호」, 「소프트식별번호」를 어떠한 정보에 의거하여 생성하는지는 임의이며, 예를 들면 「하드식별번호」를 그 휴대단말 장치의 「제조회사코드」+「제조번호」등으로 구성해도 좋다. 또 동일DB카드내에 복수의 모빌DB가 격납되어 있는 경우에 각 모빌DB마다 「소프트식별번호」를 상이시켜도 좋다.

또 단말그룹은 복수의 단말을 단순히 구분하는 이외에 1대의 단말이 복수의 그룹에 속하는 설정도 가능하다.

또 모빌DB파일을 작성할 때에 「레코드암호화키(RK)」의 값을 갱신함으로써 각각 다른 키를 이용하여 각 레코드 필드를 개별로 암호화하도록 했지만, 「레코드암호화키(RK)」를 각 레코드마다 준비해 두고, 대응하는 키를 이용하여 각 레코드를 암호화하도록 해도 좋다. 또 「레코드암호화키(RK)」를 휴대단말장치 측에 기억관리시켜도 좋다.

그 밖에 모빌DB파일내에 있어서의 FAT를 스크램블한 경우를 나타냈지만, 모빌DB파일 자체를 스크램블화하도록 해도 좋다. 또한 패스워드에 있어서도 시간변수를 키로 하여 암호화하는 경우에 한정되지 않는 것은 물론이다.

또 상기한 한 실시형태에 있어서는, 휴대형 기억매체인 DB카드로서, 콤팩트플래쉬카드를 예시했지만, 그 밖에 PC카드, 스마트미디어, CD(광디스크), MD(광자기디스크), FD(플로피디스크) 등이어도 좋고, 또한 카드형에 한정되지 않고 카세트형, 스틱형 등 그 형상은 임의이다.

또한 휴대단말장치로서는 전자수첩, 노트형 퍼스컴, PDA, 휴대전화 등이어도 좋다.

(57) 청구의 범위

청구항 1

휴대형 데이터기억매체의 이용을 제한하는 액세스제한정보로서의 제 1 식별정보 및 제 2 식별정보가 기억되어 있는 휴대단말장치이며,

임의의 휴대형 데이터기억매체를 액세스할 때에, 이 데이터기억매체내에 기억되어 있는 제 3 식별정보와 제 1 식별정보를 대조하고, 그 대조결과에 의거하여 해당 데이터기억매체에 대한 액세스가부를 결정하는 제 1 결정수단과,

해당 데이터기억매체에 대한 액세스가 허가된 경우에, 이 데이터기억매체내에 기억되어 있는 제 4 식별정보를 판독하고, 그 판독된 제 4 식별정보와 자기의 장치내에 기억되어 있는 상기 제 2 식별정보를 대조하며, 그 대조결과에 의거하여 해당 데이터기억매체내의 데이터로의 액세스가부를 결정하는 제 2 결정수단을 구비하는 것을 특징으로 하는 휴대단말장치.

청구항 2

제 1 항에 있어서,

상기 데이터기억매체는 상기 제 3 식별정보 및 제 4 식별정보 외에, 이 제 4 식별정보에 대응지워져 있는 어플리케이션소프트를 기억하고,

상기 휴대단말장치는 해당 데이터기억매체에 대한 액세스가 허가된 경우에 있어서, 이 데이터기억매체내의 어플리케이션소프트의 기동이 지시되었을 때에, 이 어플리케이션소프트에 대응지워져 있는 상기 제 4 식별정보와 상기 제 2 식별정보를 대조하고, 그 대조결과에 의거하여 해당 어플리케이션소프트를 기동하는 것을 특징으로 하는 휴대단말장치.

청구항 3

제 2 항에 있어서,

상기 데이터기억매체는 또한 상기 어플리케이션소프트에 의하여 액세스 가능한 데이터파일을 기억하고,

상기 휴대단말 장치는 이 데이터기억매체내의 어플리케이션소프트의 기동에 의거하여 그 데이터파일내에 대한 액세스처리를 실행하는 실행수단을 구비하는 것을 특징으로 하는 휴대단말장치.

청구항 4

제 1 항에 있어서,

상기 데이터기억매체에 격납되어 있는 데이터파일은 그 각 레코드가 개별로 암호화되어 있는 동시에, 이 암호화된 데이터파일의 관리정보가 해당 데이터매체대응의 휴대단말장치에 의하여 해제 가능한 형태로 스

크롬블처리되어 있는 것을 특징으로 하는 휴대단말장치.

청구항 5

제 3 식별정보와, 제 4 식별정보와, 오퍼레이터인증정보가 기억된 휴대형 데이터기억매체를 액세스하는 휴대단말장치이며,

상기 제 3 식별정보에 대응한 제 1 식별정보 및 상기 제 4 식별정보에 대응한 제 2 식별정보를 기억하는 기억수단과,

상기 데이터기억매체내에 편입되어 있는 기본소프트를 가동시켰을 때에, 이 기본소프트에 따라서 해당 데이터기억매체내에 기억되어 있는 제 3 식별정보를 판독하여 자기의 장치내에 미리 기억되어 있는 상기 제 1 식별정보와 대조하고, 그 대조결과에 의거하여 해당 데이터기억매체에 대하여 그 액세스가 허가되어 있는 정당한 단말장치인지를 체크하는 제 1 체크수단과,

정당한 단말장치인 경우에는 오퍼레이터인증정보의 입력을 받아들임 가능하게 하는 동시에 입력된 인증정보와 해당 데이터기억매체내에 기억되어 있는 상기 오퍼레이터인증정보를 대조하고, 그 대조결과에 의거하여 정당한 오퍼레이터인지를 체크하는 제 2 체크수단과,

정당한 오퍼레이터인 경우에 그 데이터기억매체내에 기억되어 있는 제 4 식별정보를 판독하여 자기의 장치내에 미리 기억되어 있는 상기 제 2 식별정보와 대조하고, 그 대조결과에 의거하여 해당 데이터기억매체내의 데이터에 대하여 그 액세스가 허가되어 있는 정당한 단말장치인지를 체크하는 제 3 체크수단을 구비하는 것을 특징으로 하는 휴대단말장치.

청구항 6

제 5 항에 있어서,

입력된 인증정보와 해당 데이터기억매체내에 기억되어 있는 오퍼레이터인증정보를 대조한 결과 인증정보의 오입력이 연속되어 복수회 반복된 경우에, 그 오입력횟수가 미리 설정되어 있는 횟수에 도달했을 때에는 기본적인 동작제어정보를 강제적으로 삭제함으로써 그 이후의 동작을 물리적으로 금지시키는 금지제어수단을 구비하는 것을 특징으로 하는 휴대단말장치.

청구항 7

휴대단말장치에 의하여 이용되어야 할 데이터파일을 휴대형 데이터기억매체에 기입하는 서버장치이며,

상기 휴대형 데이터기억매체로의 데이터파일의 기입 외에 해당 데이터기억매체와 그것을 액세스 가능한 휴대단말장치를 대응시키기 위해 해당 데이터기억매체 자체에 대한 액세스를 제한하는 제 1 식별정보 및 데이터기억매체내에 기입된 데이터파일로의 액세스를 제한하는 제 2 식별정보를 상기 휴대단말장치와 상기 휴대형 데이터기억매체에 각각 기입하는 제 1 기입수단과,

해당 휴대형 데이터기억매체와 그것을 이용 가능한 사용자를 대응시키기 위해 사용자 고유의 인증정보를 해당 휴대형 데이터기억매체에 기입하는 제 2 기입제어수단을 구비하는 것을 특징으로 하는 서버장치.

청구항 8

휴대단말장치와의 대응지움에 설정되어 있는 휴대형 데이터기억매체에 대하여 해당 휴대단말 장치에 의하여 이용되어야 할 데이터파일을 기입하는 서버장치이며,

기입대상으로서의 데이터파일내의 각 레코드를 개별로 암호화하는 수단과,

이 암호화된 데이터파일을 상기 휴대형 데이터기억매체에 대응하는 상기 휴대단말장치에 의하여 해제 가능한 형태로 스크램블처리하는 수단과,

이 스크램블처리된 데이터파일을 상기 휴대형 데이터기억매체에 기입하도록 한 기입수단을 구비하는 것을 특징으로 하는 서버장치.

청구항 9

제 8 항에 있어서,

상기 암호화 및 스크램블화된 데이터파일을 기억하는 상기 휴대형 데이터기억매체를 액세스할 때에 해당 데이터기억매체와의 대응지움에 설정된 정당한 단말장치인지를 체크하는 수단과,

정당한 단말장치이면 해당 데이터기억매체내의 데이터파일의 스크램블을 해제하고, 그 데이터파일로의 액세스를 허가하며, 액세스대상으로서 지정된 해당 데이터파일내의 암호화레코드를 개별로 판독하는 동시에, 판독한 암호화레코드를 복호화처리하여 그 레코드내용을 표시하는 수단을 구비하는 것을 특징으로 하는 서버장치.

청구항 10

휴대단말장치와, 이 휴대단말장치에 의하여 이용되는 휴대형 데이터기억매체에 데이터파일을 기입하여 배포하는 서버장치를 포함하는 시스템이며,

상기 서버장치는,

상기 휴대단말장치와의 대응지움에 설정되어 있는 상기 휴대형 데이터기억매체에 배포해야 할 데이터파일의 각 레코드를 개별로 암호화하는 암호화수단과,

이 암호화수단에 의하여 각 레코드가 개별로 암호화된 데이터파일을 해당 데이터기억매체에 기입하는 기

입수단을 구비하고,

상기 휴대단말장치는,

자기의 휴대단말 장치에 세트되어 있는 상기 휴대형 데이터기억매체가 해당 휴대단말 장치에 대응지원져 있는 정당한 매체인지를 판별하는 판별수단과,

정당한 매체인 것이 판별된 경우에 그 휴대형 데이터기억매체내의 데이터파일로의 액세스를 허가하는 액세스제어수단과,

이 액세스제어수단에 의하여 해당 휴대형 데이터기억매체내의 데이터파일로의 액세스가 허가된 경우에 액세스대상으로서 임의로 지정된 레코드를 개별로 판독하고, 이 판독한 레코드를 처리대상으로 하여 그 복호화처리와 복호화된 레코드내용을 표시하는 레코드출력처리를 실행하는 레코드처리수단을 구비하는 것을 특징으로 하는 시스템.

청구항 11

제 10 항에 있어서,

상기 레코드처리수단은 복호화처리에 의하여 복호화된 레코드내용을 단말내의 일시기억메모리에 기억시키고, 상기 데이터파일로에 대한 액세스처리의 종료, 또는 그 단말처리종료에 의해 상기 일시기억메모리내의 복호화레코드를 소거하는 것을 특징으로 하는 시스템.

청구항 12

제 10 항에 있어서,

상기 암호화수단은 데이터파일의 각 레코드를 개별로 암호화하는 동시에, 그 레코드내의 각 필드를 개별로 암호화하고,

상기 레코드처리수단은 상기 휴대형 데이터기억매체내의 데이터파일을 액세스할 때에, 액세스대상으로서 임의로 입력된 키를 암호화하는 동시에, 암호화되어 있는 데이터파일의 각 레코드를 상기 암호화된 키에 의거하여 검색함으로써 입력키에 해당하는 필드를 갖는 레코드를 개별로 판독하고, 이 판독한 레코드를 처리대상으로 하여 그 복호화처리와 복호화된 레코드내용을 표시하는 레코드출력처리를 실행하는 것을 특징으로 하는 시스템.

청구항 13

제 10 항에 있어서,

상기 레코드처리수단은 상기 휴대형 데이터기억매체내의 데이터파일로부터 개별로 판독하여 그것을 복호화한 레코드에 대해서 그 변경이 지시되거나, 또는 해당 데이터파일로에 대하여 신규레코드의 추가가 지시된 경우에, 그 변경된 레코드, 또는 추가된 레코드를 암호화하는 동시에, 암호화된 레코드를 상기 데이터파일로에 대한 갱신정보로서 해당 휴대형 데이터기억매체내에 기입하는 것을 특징으로 하는 시스템.

청구항 14

컴퓨터가 판독 가능한 프로그램코드를 갖는 기록매체이며,

서버장치에 대하여 휴대단말장치와의 대응지음이 설정되어 있는 휴대형 데이터기억매체에 배포해야 할 데이터파일의 각 레코드를 개별로 암호화시키는 컴퓨터가 판독 가능한 프로그램코드와,

각 레코드가 개별로 암호화된 데이터파일을 해당 데이터기억매체에 기입시키는 컴퓨터가 판독 가능한 프로그램코드와,

휴대단말장치에 대하여 그것에 세트되어 있는 데이터기억매체가 해당 단말에 대응지원져 있는 정당한 매체인지를 판별시키는 컴퓨터가 판독 가능한 프로그램코드와,

단말대응의 매체인 것이 판별된 경우에, 그 데이터기억매체내의 데이터파일로의 액세스를 허가시키는 컴퓨터가 판독 가능한 프로그램코드와,

데이터기억매체내의 데이터파일로의 액세스가 허가된 경우에 액세스대상으로서 임의로 지정된 레코드를 개별로 판독하고, 이 판독한 레코드를 처리대상으로 하여 그 복호화처리와 복호화된 레코드내용을 표시하는 레코드출력처리를 실행시키는 컴퓨터가 판독 가능한 프로그램코드를 갖는 것을 특징으로 하는 기록매체.

청구항 15

휴대단말장치와, 이 휴대단말장치에 의하여 이용되는 휴대형 데이터기억매체에 데이터파일을 기입하여 배포하는 서버장치를 갖는 시스템이며,

상기 서버장치는,

상기 휴대단말장치에서 이용되는 레코드군을 마스터데이터파일로부터 잘라내고, 그 잘라낸 레코드군으로부터 모빌데이터파일을 작성하는 모빌데이터작성수단과,

상기 휴대단말장치와의 대응지음이 설정되어 있는 상기 휴대형 데이터기억매체에 상기 모빌데이터작성수단에 의하여 작성된 모빌데이터파일을 기입하는 기입수단을 구비하고,

상기 휴대단말장치는,

자기의 단말장치에 세트되어 있는 상기 휴대형 데이터기억매체가 해당 단말에 대응지원져 있는 정당한 매

체인지를 판별하는 판별수단과,

이 판별수단에 의하여 해당 단말대응의 매체인 것이 판별된 경우에, 그 데이터기억매체내의 모빌데이터파일로의 액세스를 허가하는 액세스제어수단을 구비하는 것을 특징으로 하는 시스템.

청구항 16

제 15 항에 있어서,

상기 모빌데이터작성수단은 상기 휴대단말장치에서 이용되는 레코드군을 마스터데이터파일로부터 잘라낼 때에, 그 휴대단말장치측에서의 처리내용에 맞추어서 미리 설정되어 있는 레코드추출조건을 참조하고, 이 레코드추출조건에 합치하는 레코드군을 잘라내는 것을 특징으로 하는 시스템.

청구항 17

제 15 항에 있어서,

상기 모빌데이터작성수단은 상기 휴대단말장치에서 이용되는 레코드군을 마스터데이터파일로부터 잘라내어 모빌데이터파일을 작성할 때에, 그 휴대단말장치측에서의 처리내용에 맞추어서 미리 설정되어 있는 추출대상필드를 참조하고, 이 추출대상필드의 조건에 합치하는 필드만으로 이루어지는 레코드구성의 모빌데이터파일을 작성하는 것을 특징으로 하는 시스템.

청구항 18

제 15 항에 있어서,

상기 모빌데이터작성수단은 상기 휴대단말장치에서 이용되는 레코드군을 마스터데이터파일로부터 잘라낼 때에 기입대상인 상기 휴대형 데이터기억매체내에 설정되어 있는 식별정보를 취득하고, 이 식별정보에 의거하여 마스터데이터파일을 결정하는 동시에, 이 마스터데이터파일로부터 레코드군을 잘라내기 위한 잘라낼조건을 결정하고, 결정한 마스터데이터파일로부터 그 잘라낼조건에 따라서 레코드군의 잘라냄을 실시하는 것을 특징으로 하는 시스템.

청구항 19

휴대단말장치에 의하여 이용되는 휴대형 데이터기억매체에 모빌데이터파일을 기입하여 배포하는 서버장치

는,
모빌데이터파일을 처리하기 위한 어플리케이션소프트가 해당 모빌데이터파일에 대응지원서 데이터기억매체내에 기억되어 있는지를 판별하는 판별수단과,

이 판별수단에 의하여 그 어플리케이션소프트가 기억되어 있지 않은 것이 판별된 경우에는 해당 모빌데이터파일에 대응지원서 그것을 처리하기 위한 어플리케이션소프트를 해당 휴대형 데이터기억매체에 기입하는 수단을 구비하는 것을 특징으로 하는 서버장치.

청구항 20

제 19 항에 있어서,

상기 데이터기억매체내에 모빌데이터파일에 대응지원서 그 어플리케이션소프트가 기억되어 있는 경우에, 그 어플리케이션소프트는 최신의 것인지를 판별하는 판별수단과,

이 판별수단에 의하여, 최신의 어플리케이션소프트는 아닌 것이 판별된 경우에 상기 휴대형 데이터기억매체내에 모빌데이터파일에 대응지원서 기억되어 있는 어플리케이션소프트를 최신의 어플리케이션소프트로 개서하는 어플리케이션결신수단을 추가로 구비하는 것을 특징으로 하는 서버장치.

청구항 21

컴퓨터가 판독 가능한 프로그램코드를 갖는 기록매체이며,

휴대단말장치에 의하여 이용되는 휴대형 데이터기억매체에 데이터파일을 기입하여 배포하는 서버 장치에 대하여,

휴대단말장치에서 이용되는 레코드군을 마스터데이터파일로부터 잘라내고, 그 잘라낸 레코드군으로부터 모빌데이터파일을 작성시키는 컴퓨터가 판독 가능한 프로그램코드와,

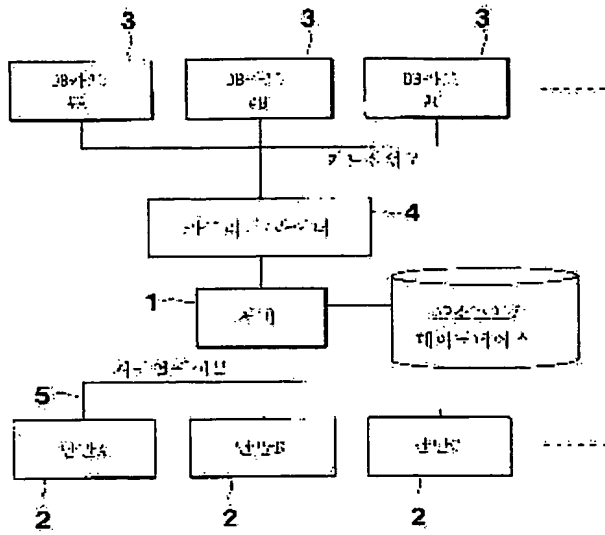
휴대단말장치와의 대응지움에 설정되어 있는 데이터기억매체에 상기 모빌데이터파일을 기입시키는 컴퓨터가 판독 가능한 프로그램코드와,

휴대단말장치에 대하여 그것에 세트되어 있는 데이터기억매체가 해당 단말에 대응지원져 있는 정당한 매체인지를 판별시키는 컴퓨터가 판독 가능한 프로그램코드와,

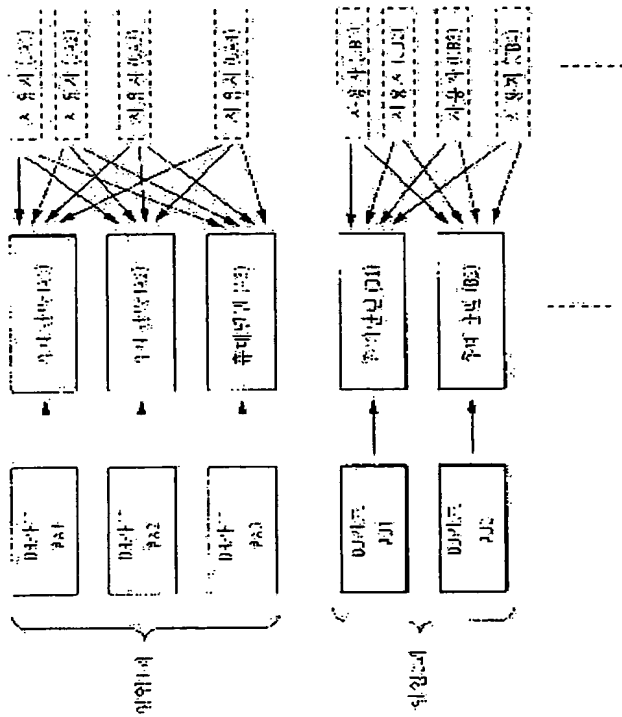
해당 단말대응의 매체인 것이 판별된 경우에, 그 데이터기억매체내의 모빌데이터파일로의 액세스를 허가시키는 컴퓨터가 판독 가능한 프로그램코드를 갖는 것을 특징으로 하는 기록매체.

도면

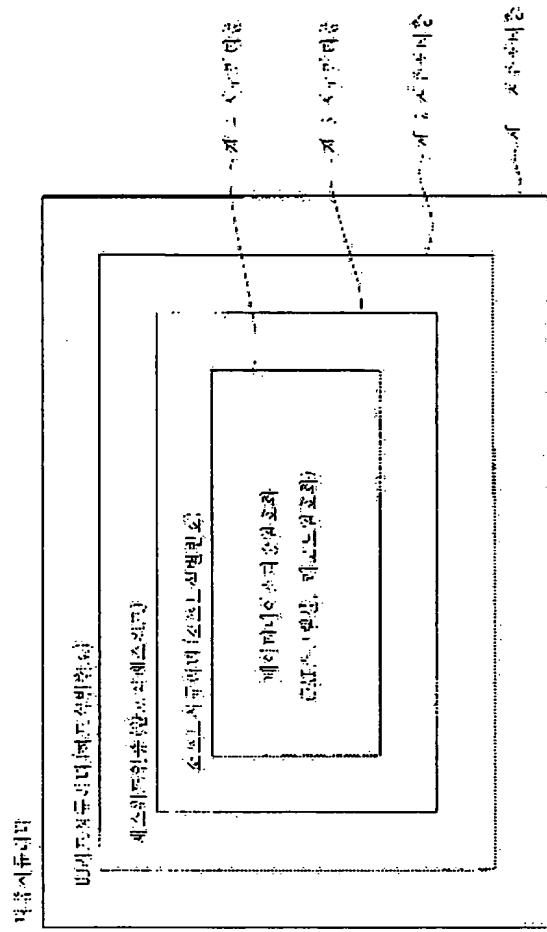
도면1



도면2



도 3



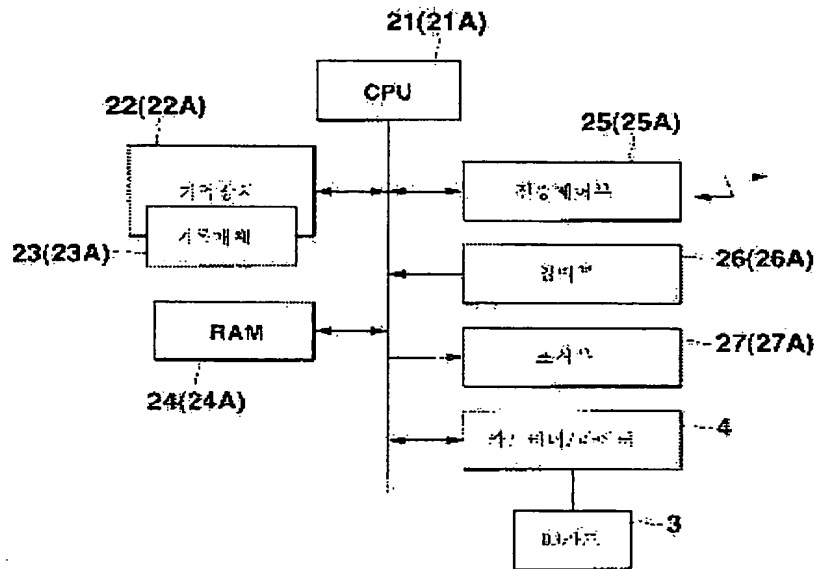
도면8

내장하드디스크 구성

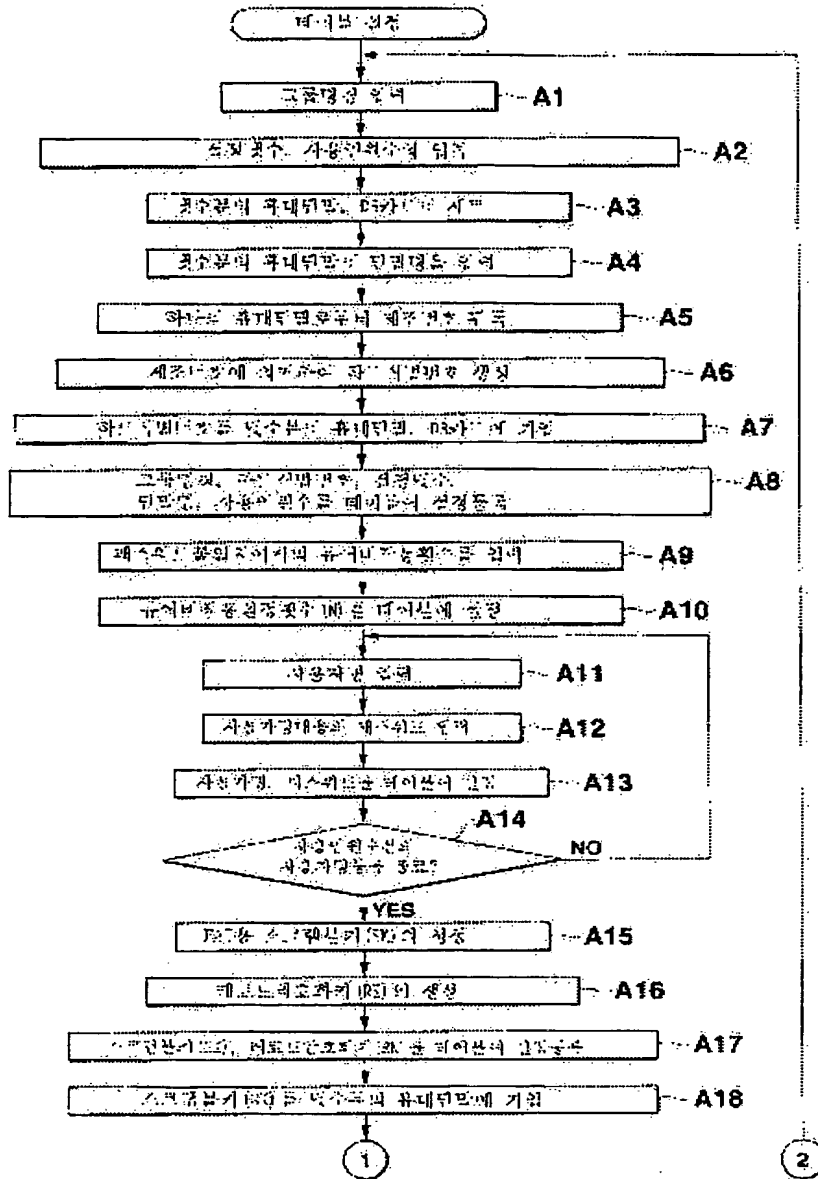
| | |
|---------------|--|
| -디스크명 | |
| 주요 디스크명 | |
| 수용용 디스크명 | |
| 소속명(부속) | |
| 400 (인사/인사부서) | |
| 기타 디스크명(인사부서) | |
| 소속명(인사부서) | |
| 소속명(인사부서) | |
| 기타 | |

도면7

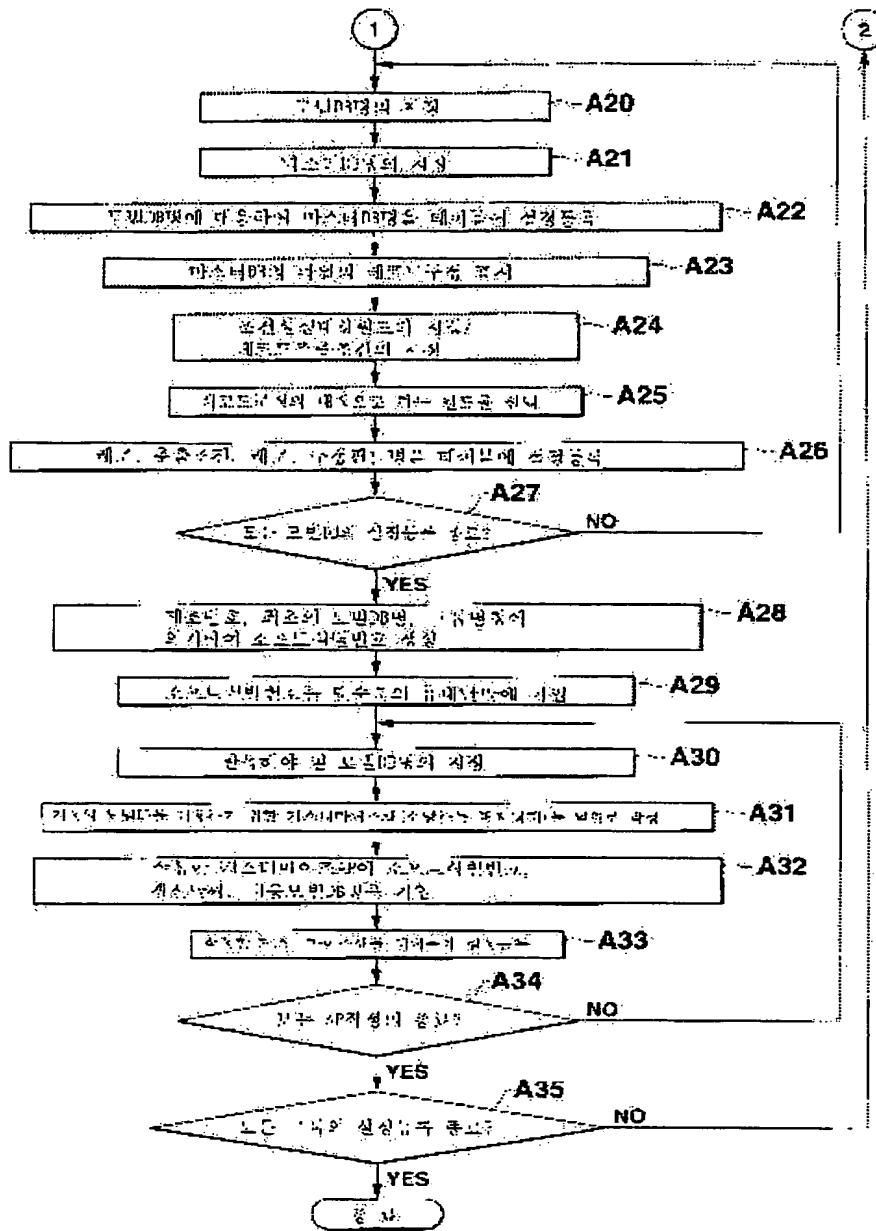
기타/인사부서 구성



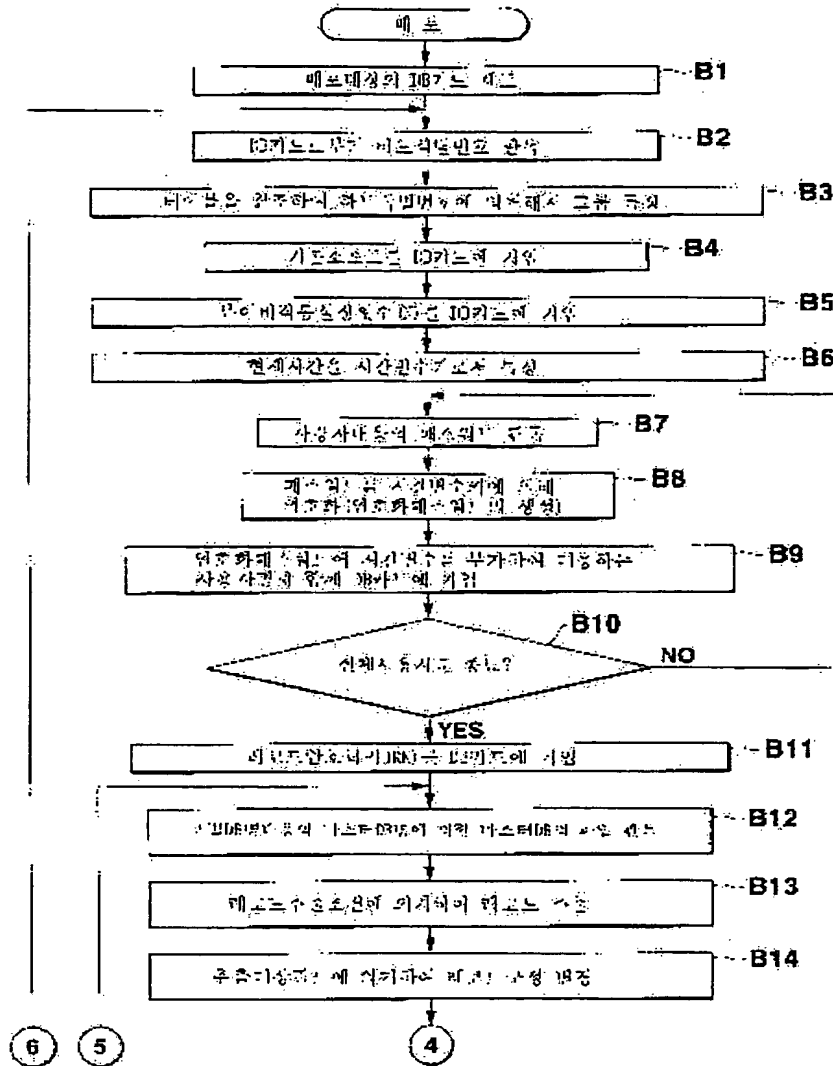
도 8a



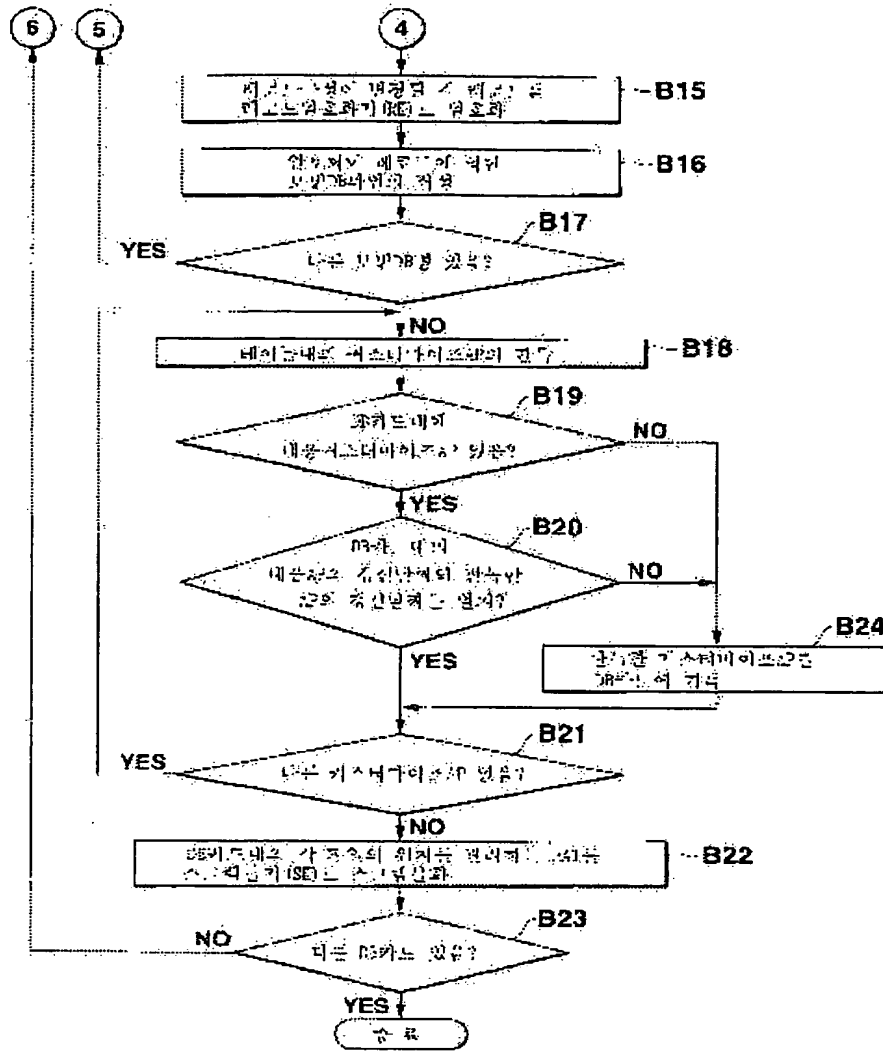
도 8b



도면 6a



도면 9b



도면 10a

제 10표

| | 이름 | 주소 | 신뢰번호 | 배치 이노베이션 | 서명 | 직책명 | 원년 | 생년월일 |
|----|-----|----|------|-------------|----|-----|----|------------|
| 1 | 김민준 | | | | | | | 10/01/ '99 |
| 2 | 김민준 | | | | | | | 10/15/ '99 |
| 3 | 김민준 | | | | | | | 10/30/ '99 |
| 4 | 김민준 | | | | | | | 11/25/ '99 |
| 5 | 김민준 | | | | | | | 12/20/ '99 |
| 6 | 김민준 | | | | | | | 01/15/ '00 |
| 7 | 김민준 | | | | | | | 01/28/ '00 |
| 8 | 김민준 | | | | | | | 02/10/ '00 |
| 9 | 김민준 | | | | | | | 02/20/ '00 |
| 10 | 김민준 | | | | | | | 03/10/ '00 |

도면 10b

표 10a 참조

| | 이름 | 주소 | 전화번호 | 기술 이력 | 성별 | 보안관 | 인명 | 경신일자 |
|---|------|----|------|----------|----|-----|----|----------|
| 1 | FAA | | | | | | | 01/15/00 |
| 2 | FAA | | | | | | | 01/28/00 |
| 3 | IR-E | | | | | | | 02/10/00 |
| 4 | AT | | | | | | | 02/20/00 |
| 5 | FAA | | | | | | | 03/10/00 |

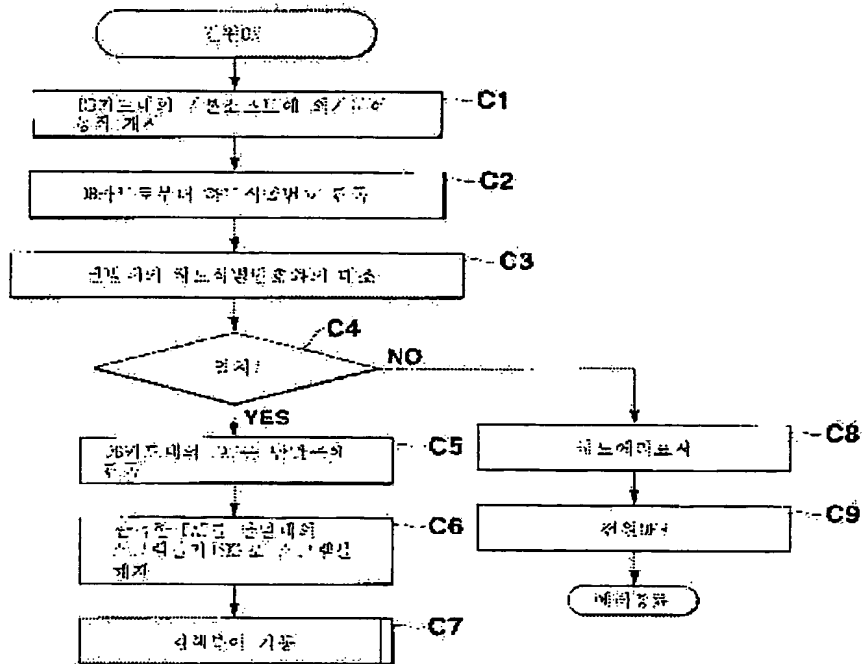
도면 10c

테스트구분 표시

| | 이름 | 주소 | 전화 | 인명 |
|---|------|----|----|----|
| 1 | FAA | | | |
| 2 | FAA | | | |
| 3 | IR-E | | | |
| 4 | AT | | | |
| 5 | FAA | | | |

도면 10a 참조

도면 11



도면 12

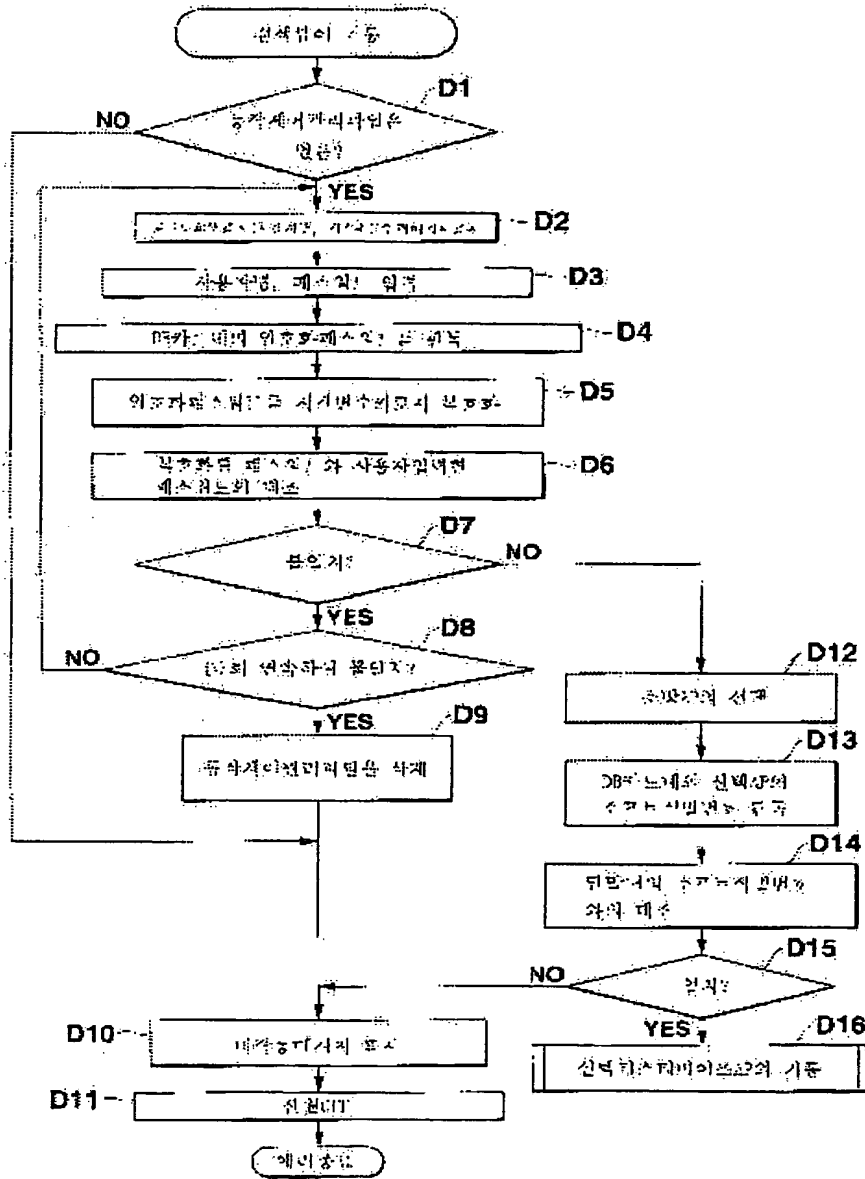
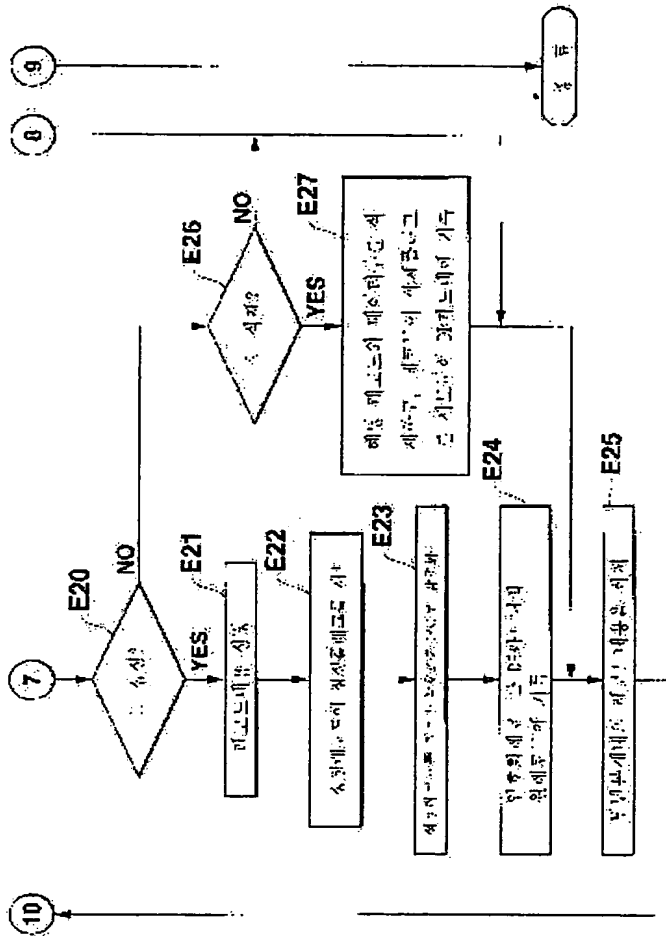
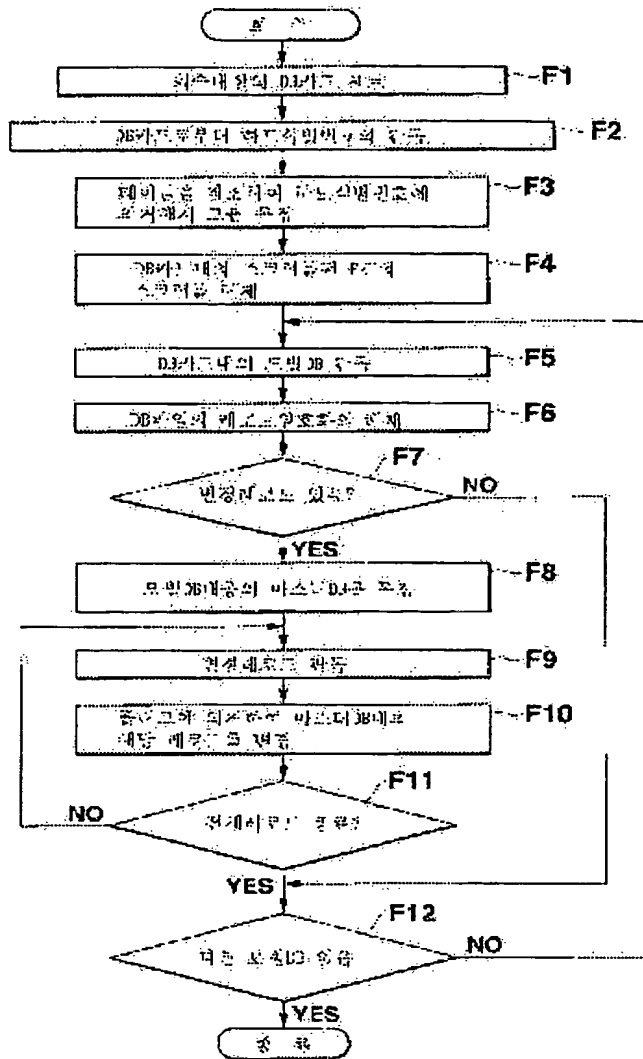




도표 136



도면 14



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.